



Tivoli Public Key Infrastructure

Anpassung

Version 3 Release 7.1

SH12-3000-02



Tivoli Public Key Infrastructure

Anpassung

Version 3 Release 7.1

SH12-3000-02

Copyrightvermerke

Copyright © 1999, 2001 IBM Corp., einschließlich dieser Dokumentation und aller Software. Alle Rechte vorbehalten. Kann nur gemäß der Softwarelizenzvereinbarung von Tivoli Systems bzw. IBM oder dem Anhang für Tivoli-Produkte der IBM Nutzungsbedingungen verwendet werden. Diese Veröffentlichung darf ohne vorherige schriftliche Genehmigung der IBM Corp. weder ganz noch in Auszügen auf irgendeine Weise - elektronisch, mechanisch, magnetisch, optisch, chemisch, manuell u. a. - vervielfältigt, übertragen, aufgezeichnet, auf einem Abrufsystem gespeichert oder in eine andere Computersprache übersetzt werden. Die IBM Corp. gestattet Ihnen in begrenztem Umfang, eine Hardcopy oder eine Reproduktion einer maschinenlesbaren Dokumentation für den eigenen Gebrauch zu erstellen, unter der Voraussetzung, dass jede dieser Reproduktionen mit dem Copyrightvermerk der IBM Corp. versehen ist. Weitere das Copyright betreffende Rechte werden nur nach vorheriger schriftlicher Genehmigung durch die IBM Corp. gewährt. Die Veröffentlichung dient nicht zu Produktionszwecken. **Die in diesem Dokument aufgeführten Beispiele sollen lediglich zur Veranschaulichung und zu keinem anderen Zweck dienen.**

Marken

AIX, DB2, DB2 Universal Database, IBM, RS/6000, SecureWay, Tivoli and WebSphere sind in gewissen Ländern eingetragene Marken der International Business Machines Corp. oder von Tivoli Systems Inc.

Das Programm Tivoli PKI (im folgenden als "Programm" bezeichnet) enthält Komponenten von IBM WebSphere Application Server und IBM HTTP Web Server ("IBM Server"). Diese dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Das Programm Tivoli PKI (im folgenden als "Programm" bezeichnet) enthält Komponenten von DB2 Universal Database. Diese Komponenten dürfen nur zusammen mit dem Programm installiert und entsprechend der für das Programm geltenden Lizenzvereinbarungen in Kombination mit diesem verwendet werden, um Daten zu speichern und zu verwalten, die vom Programm verwendet oder generiert werden. Für andere Datenverwaltungsoperationen ist der Einsatz nicht gestattet. Diese Lizenz gilt z. B. nicht für eingehende Verbindungen zur Datenbank, die von anderen Anwendungen aus für Abfragen und Berichtserstellungsoperationen hergestellt werden. Sie sind lediglich zur Installation und Verwendung dieser Komponenten auf der gleichen Maschine berechtigt, auf der auch das Programm installiert und verwendet wird.

Das Programm enthält Komponenten des IBM WebSphere Application Server und des IBM HTTP Web Server ("IBM Server"). Sie sind nicht berechtigt, die IBM Server zu anderen Zwecken als in Verbindung mit der lizenzgerechten Verwendung des Programms zu benutzen. Die IBM Server müssen auf derselben Maschine wie das Programm installiert sein. Sie sind nicht berechtigt, sie unabhängig vom Programm zu installieren und zu verwenden.

Java und alle auf Java basierenden Marken und Logos sind in gewissen Ländern Marken der Sun Microsystems, Inc.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

UNIX ist eine eingetragene Marke und wird ausschließlich von der X/Open Company Limited lizenziert.

Pentium ist in gewissen Ländern eine Marke der Intel Corporation.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden. Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, daß nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme und Dienstleistungen in Verbindung mit Fremdprodukten liegt beim Kunden, soweit solche Verbindungen nicht ausdrücklich von IBM bestätigt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France, zu richten. Anfragen an obige Adresse müssen auf englisch formuliert werden.



Dieses Programm enthält Sicherheitssoftware von RSA Data Security, Inc. Copyright © 1994 RSA Data Security, Inc. Alle Rechte vorbehalten.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Hewlett-Packard Company. Copyright (c) 1994.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Hewlett-Packard Company macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Dieses Programm enthält STL-Software (STL = Standard Template Library) von Silicon Graphics Computer Systems, Inc. Copyright (c) 1996 - 1999.

- Die Berechtigung zum Verwenden, Kopieren, Ändern, Verteilen und Verkaufen dieser Software sowie der zugehörigen Dokumentation für die gewünschten Zwecke wird hiermit gebührenfrei erteilt. Voraussetzung hierfür ist allerdings, daß der o. a. Copyrightvermerk auf allen Kopien erscheint, und daß sowohl dieser Copyrightvermerk als auch dieser Berechtigungshinweis in der zugehörigen Dokumentation aufgeführt werden. Silicon Graphics macht keine Angaben zur Eignung dieser Software für bestimmte Zwecke. Sie wird ohne Modifikationen und ohne Gewährleistung bereitgestellt.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Inhaltsverzeichnis

Vorwort	ix
Zielgruppe	ix
Referenzinformationen	ix
Inhalt des Handbuchs	x
In diesem Handbuch verwendete Konventionen.	xi
Kundenunterstützung anfordern.	xi
Tivoli PKI - Webinformationen.	xi
 Kapitel 1. Informationen zu Tivoli PKI	 1
 Kapitel 2. Übersicht.....	 3
 Kapitel 3. Informationen zur Vorgehensweise.....	 5
Planen der Anpassung	5
Editieren anpassbarer Dateien	6
Anpassen der Registrierung	6
Directory-Einträge während der Registrierung erstellen	6
Hinzufügen eines Registrierungsfelds.	7
Hinzufügen eines Werts zu einer Auswahlliste	8
Ändern von Bildmaterial auf einer Registrierungsseite	9
Ändern von Text auf einer Registrierungsseite	9
Ändern von Text im Benachrichtigungsbrief.	9
Herstellen einer Verbindung zur Registrierung über eine andere URL-Adresse	10
Aktivieren der automatischen Anforderungsverarbeitung.	10
Aktivieren der E-Mail-Benachrichtigung unter Windows NT	10
Anpassen des Regel-Exits	11
Identifizieren des Regel-Exit-Namens.	11
Ändern des Beispiel-Regel-Exits	11
Ersetzen des Beispiel-Regel-Exits	12
Anpassen von Zertifikaten	12
Hinzufügen eines Zertifikatsprofils.	13
Hinzufügen der Beschreibung eines Zertifikatstyps.	13
Ändern eines Zertifikatsprofils.	13
Ändern der Beschreibung eines Zertifikatstyps.	14
Ändern des Anzeigenamens eines Zertifikatstyps	14
Löschen eines Zertifikatsprofils	15
Löschen der Beschreibung eines Zertifikatstyps	15
Hinzufügen von Benutzererweiterungen zu einem Zertifikatsprofil	15

Ändern der angezeigten URL-Adresse nach Verlassen von RA Desktop	16
Anpassen der Sicherung und Wiederherstellung von Schlüsseln	16
Inaktivieren der Sicherung und Wiederherstellung von Schlüsseln.....	16
Ändern der Anforderungsinformationen	17
Aktivieren der automatischen Genehmigung.....	17

Kapitel 4. Erläuterungen 19

Anpassung	19
Anpassbare Elemente.....	19
Änderungen, die einen Systemwiederanlauf erfordern.....	19
Registrierung.....	19
Registrierungsfunktion.....	20
Registrierungswebseiten.....	20
Vorabregistrierung	21
Webbrowserunterstützung	21
Regel-Exits	21
Einschränkungen bei Regel-Exits.....	21
Schnittstellen zum Regel-Exit	22
Registrierung.....	23
Unternehmensregel	23
Datensatzattribute	24
Registrierungsstellen	24
Registrierungsdatenbanken.....	24
Registrierungsdomänen	24
Registrierungssätze	25
Zertifizierung	25
Zertifikatsaussteller	26
Zertifikatswiderrufslisten (CRL).....	26
Verzeichnisse (Directory).....	26
Registrierte Namen	26
Zertifikate	27
Browserzertifikate	27
CA-Zertifikate.....	27
Server- oder Einheitenzertifikate	28
Zertifikatserweiterungen.....	28
Erneuerbarkeit.....	28
Zertifikatsprofile	29
Profilverarbeitung	30
Organisation, Inhalt und Struktur von Profilen	32

Substitutionsvariablen in Profilen	33
Profilregeln und -definitionen	35
Verwaltung	38
Zugriffssteuerung	38
Authentifizierung und Berechtigung	39
Parallele Verwaltung	39
RA Desktop	39
Servlet zur Unterstützung von RA Desktop	39
Anforderungsprofile	40
Funktion zur Sicherung und Wiederherstellung von Schlüsseln	40
Kapitel 5. Referenzinformationen	41
Anpassungs-Tools	41
Dateiadressen	42
Verzeichnisstruktur	42
Anpassbare Elemente	42
Quellendateien auf den Webseiten	43
Beispieldateien	44
Beschreibungsdateien für Zertifikatstypen	44
Konfigurationsdatei für Zertifikatsprofile	45
E-Mail-Benachrichtigungsbrief	46
Fehlernachrichtentext	47
Java Server-Seite (JSP)	48
Regel-Exit-Datei	49
Konfigurationsdatei für die Registrierungsfunktion	51
Einzelangaben auf den Webseiten	56
Registrierungsformularvariablen	56
Widerrufsgründe	62
Einzeldaten von Zertifikaten	62
Zertifikatstypen	62
Benutzerdefinierte Erweiterungen	64
Format von X.509v3-Zertifikaten	64
Einzelangaben bei der Registrierung	65
Attribute von Anforderungen und Zertifikaten	65
RA-Aktionen	66
Status der Registrierungsanforderungen	67
Kapitel 6. Anpassungsbeispiel	69
Planen der Anpassung	69

Verzeichnisstruktur des Unternehmens	69
Identifizieren der kundenspezifischen Anforderungen	70
Identifizieren der zu ändernden Dateien	71
Änderungen vornehmen	72
Webseiten: Seitentitel und -beschreibungen ändern	73
Sammeln von unternehmensbezogenen Kunden- und Mitarbeiterdaten	102
Überprüfen persönlicher Daten	105
Angaben der Seite, die nach dem Herunterladen des Zertifikats aufgerufen werden soll.	107
Grafiken ersetzen	107
Aktualisieren des Benachrichtigungsbriefs	108
Ändern von Zertifikatstypen	109
Hinzufügen von Werten zu Auswahllisten	111
Verarbeiten von Genehmigungen	112
Verzeichnis-Server anpassen	113
Anpassen von Objektklassen für Verzeichniseinträge (Directory)	114
Änderungen prüfen	115
Glossar	117
Index	137

Vorwort

Dieses Buch enthält Informationen dazu, wie Sie die Tivoli PKI-Registrierungsfunktion für die Unterstützung der Registrierungs- und Zertifizierungsziele Ihrer Unternehmensregeln anpassen können.

Dieses Release des Produkts unterstützt lediglich AIX-Plattformen. Alle Materialien, die sich mit Microsoft Windows befassen, sollten ignoriert werden.

Zielgruppe

Dieses Buch richtet sich an Anwendungsentwickler und Systemadministratoren, die bestimmte Aspekte von Tivoli PKI an die individuellen Bedürfnisse ihres Unternehmens anpassen wollen. So können beispielsweise HTML-Seiten, Zertifikatsprofile, Regel-Exits und Benachrichtigungsbriefe angepasst werden.

Benutzer dieses Handbuchs sollten sich in der Verwendung der unterstützten Internetbrowser auskennen und über Erfahrung mit e-business-Anwendungen verfügen.

Referenzinformationen

Die Tivoli PKI-Produktdokumentation steht im PDF- (Portable Document Format) sowie im HTML-Format auf der Tivoli-Website zur Verfügung. HTML-Versionen für einige Veröffentlichungen werden zusammen mit dem Produkt installiert. Auf diese kann über die Benutzerschnittstellen zugegriffen werden.

Bitte beachten Sie, dass am Produkt selbst seit der Erstellung der Veröffentlichungen möglicherweise Änderungen vorgenommen wurden. Die neuesten Produktinformationen sowie Informationen für den Zugriff auf Veröffentlichungen in den von Ihnen gewünschten Sprachen und Formaten enthalten die Release-Informationen. Die neueste Version der Release-Informationen steht auf der Tivoli Public Key Infrastructure-Website zur Verfügung:

<http://www.tivoli.com/support>

Die Tivoli PKI-Bibliothek umfasst die folgenden Dokumentationen:

Einführung

Dieses Buch enthält eine Übersicht über das Produkt. Es enthält eine Aufstellung der Produktvoraussetzungen, Erläuterungen zu den Installationsverfahren und Informationen über den Zugriff auf die Onlinehilfefunktion für alle Produktkomponenten. Dieses Buch wird in gedruckter Form zusammen mit dem Produkt ausgeliefert.

Systemverwaltung

Dieses Handbuch enthält Basisinformationen zur Verwaltung eines Tivoli PKI-Systems. Es beschreibt die Prozeduren zum Starten und Stoppen der Server, zum Ändern von Kennwörtern, zur Verwaltung der Serverkomponenten, zum Erstellen von Protokollen sowie zur Ausführung von Datenintegritätsüberprüfungen.

Konfiguration

Dieses Handbuch enthält Informationen zur Verwendung von Setup Wizard zum Konfigurieren eines Tivoli PKI-Systems. Während Sie die Onlinehilfefunktion für diesen Assistenten anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

RA Desktop

Dieses Handbuch enthält Informationen zur Verwendung von RA Desktop für die Verwaltung von Zertifikaten während ihres Gültigkeitszeitraums. Während Sie die Onlinehilfefunktion für den Desktop anzeigen, können Sie auf die HTML-Version dieses Handbuchs zugreifen.

Benutzerhandbuch

Dieses Handbuch enthält Informationen zum Abrufen und Verwalten von Zertifikaten. Es beschreibt die Prozeduren zur Verwendung der Browserregistrierungsformulare von Tivoli PKI, um Zertifikate anzufordern, zu erneuern und zu widerrufen. Außerdem enthält es eine Erläuterung der Vorabregistrierung für PKIX-kompatible Zertifikate.

Anpassung

Dieses Buch enthält Informationen dazu, wie Sie die Tivoli PKI-Registrierungsfunktion für die Unterstützung der Registrierungs- und Zertifizierungsziele Ihrer Unternehmensregeln anpassen können. So erhalten Sie beispielsweise Anweisungen zur Anpassung von HTML- und Java Server-Seiten, Benachrichtigungsschreiben, Zertifikatsprofilen und Regel-Exits.

Die Website von Tivoli PKI enthält weitere Dokumente, die Sie bei der Installation, Verwaltung und Verwendung von Tivoli PKI unterstützen. So finden Sie hier beispielsweise zusätzliche Richtlinien zum Directory-Schema und erfahren, wie Tivoli PKI mit dem IBM SecureWay 4758 PCI Cryptographic Coprocessor integriert werden kann.

Inhalt des Handbuchs

Dieses Handbuch enthält folgende Informationen:

- „Informationen zu Tivoli PKI“ auf Seite 1 liefert eine kurze Beschreibung der Funktionen und des Leistungsspektrums von Tivoli PKI.
- „Übersicht“ auf Seite 3 beschreibt den Anpassungsprozess und erläutert Bereiche von Tivoli PKI, die angepasst werden können.
- „Informationen zur Vorgehensweise“ auf Seite 5 enthält Task-orientierte Informationen und Anleitungen zur Anpassung von Tivoli PKI.
- „Erläuterungen“ auf Seite 19 enthält Basisinformationen zu Tivoli PKI und Konzepten, die mit den Anpassungs-Tasks in Zusammenhang stehen.
- „Referenzinformationen“ auf Seite 41 enthält Felddescriptions, Werte und Attribute, die bei der Anpassung der Registrierungsfunktion eine Rolle spielen können.
- „Anpassungsbeispiel“ auf Seite 69 erläutert die Vorgehensweise beim Anpassen verschiedener Aspekte von Tivoli PKI. Anhand eines Beispielszenarios und von Mustercodes wird gezeigt, wie entsprechende Änderungen vorgenommen werden.
- „Glossar“ auf Seite 117 definiert die Termini und Abkürzungen, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt sind, sowie Termini, die von Bedeutung sein könnten.

In diesem Handbuch verwendete Konventionen

In diesem Handbuch werden für bestimmte Termini und Aktionen verschiedene Konventionen hinsichtlich des Schriftbilds verwendet. Die Schriftbilder haben folgende Bedeutung:

Schriftbild	Bedeutung
Fettdruck	Befehle, Schlüsselwörter, Markierungen und andere Informationen, die im genauen Wortlaut verwendet werden müssen, werden fett gedruckt.
<i>Kursivdruck</i>	Variablen, die angegeben werden müssen, sowie neue Termini werden <i>kursiv</i> gedruckt. Hervorgehobene Wörter und Ausdrücke werden ebenfalls <i>kursiv</i> gedruckt.
Monospace-Schrift	Codebeispiele, Ausgabe und Systemnachrichten werden in einer Monospace-Schrift gedruckt.

Kundenunterstützung anfordern

Wenn mit irgendeinem Tivoli-Produkt Probleme auftreten, können Sie über **<http://www.support.tivoli.com>** die Homepage der Tivoli-Unterstützung (Tivoli Support) aufrufen. Nachdem Sie eine Verbindung zum Kundenregistrierungsformular hergestellt und dieses übergeben haben, können Sie auf eine Reihe von Kundenunterstützungsservices auf dem Web zugreifen.

Kunden in Deutschland, Österreich oder der Schweiz können eine der folgenden Telefonnummern anrufen:

- Deutschland: **01805-00-1242**
- Österreich: **01-1706-6000**
- Schweiz: **0800-555454**

Ihre Meinung zu Tivoli-Produkten und der Tivoli-Dokumentation interessiert uns. Gerne nehmen wir Verbesserungsvorschläge Ihrerseits entgegen. Falls Sie Kommentare oder Anregungen zur vorliegenden Dokumentation haben, senden Sie uns bitten eine E-Mail an folgende Adresse: pubs@tivoli.com.

Tivoli PKI - Webinformationen

Kunden von Tivoli und IBM Tivoli finden Onlineinformationen zu allen Tivoli-Sicherheitsprodukten und Tivoli PKI.

Um wichtige Informationen über kurzfristigen Produktaktualisierungen oder Serviceinformationen zu Tivoli PKI abzurufen, beginnen Sie auf folgender Website:
http://www.tivoli.com/support/secure_download_bridge.html

Informationen zum Produkt Tivoli Public Key Infrastructure erhalten Sie auf folgender Website: **http://www.tivoli.com/products/index/secureway_public_key/**

Informationen zu anderen Sicherheitsverwaltungsprodukten von Tivoli erhalten Sie unter folgender Webadresse: **<http://www.tivoli.com/products/solutions/security/>**

1

Informationen zu Tivoli PKI

Tivoli Public Key Infrastructure stellt Anwendungen zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation bereit:

- Das Produkt ermöglicht Organisationen und Unternehmen das Ausstellen, Publizieren und Verwalten digitaler Zertifikate in Übereinstimmung mit ihren Registrierungs- und Zertifizierungsregeln.
- Unterstützung für die Verschlüsselungsstandards Public Key Infrastructure für X.509 Version 3 (PKIX) und Common Data Security Architecture (CDSA) zur Realisierung der Interoperabilität zwischen verschiedenen Lieferanten und Herstellern.
- Digitale Unterzeichnung und gesicherte Protokolle zur Authentifizierung aller an einer Transaktion beteiligten Parteien.
- Optimale Flexibilität durch browser-basierte Registrierungsfunktionen.
- Unterstützung zur Gewährleistung der Vertraulichkeit durch verschlüsselte Kommunikation und gesicherte Speicherung der Registrierungsinformationen.

Ein Tivoli PKI-System kann auf Serverplattformen unter IBM AIX/6000[®] sowie Microsoft Windows NT ausgeführt werden. Es umfasst die folgenden Hauptmerkmale:

- Ein zuverlässiger Zertifikatsaussteller (CA) verwaltet die Gültigkeitsdauer digitaler Zertifikate. Um für die Authentizität eines Zertifikats zu bürgen, leistet der CA für jedes Zertifikat, das er ausstellt, eine digitale Unterschrift. Außerdem unterzeichnet er Zertifikatswiderrufslisten (CRLs), um zu bestätigen, dass ein bestimmtes Zertifikat nicht mehr gültig ist. Zur weiteren Sicherung seines Signierschlüssels können Sie kryptografische Hardware wie beispielsweise den IBM SecureWay 4758 PCI Cryptographic Coprocessor verwenden.
- Eine Registrierungsstelle (RA) bearbeitet die Verwaltungs-Tasks für die Benutzerregistrierung. Die RA stellt sicher, dass nur solche Zertifikate ausgestellt werden, die Ihre Unternehmensaktivitäten unterstützen, und dass diese Zertifikate nur an berechtigte Benutzer ausgegeben werden. Die Verwaltungsaufgaben können über automatisierte Prozesse oder auf der Basis menschlicher Entscheidungen ausgeführt werden.
 Ähnlich wie der CA können Sie die Hardware der Einheit IBM 4758 verwenden, um die Signierschlüssel der RA zu speichern.
- Eine Webschnittstelle für die Registrierung vereinfacht das Abrufen von Zertifikaten für Browser, Server und andere Einheiten und Zwecke, z. B. VPN-Einheiten (VPN = Virtual Private Network), Smart Cards und die sichere Übertragung von E-Mails.

-
- Eine Webverwaltungsschnittstelle, Tivoli PKI RA Desktop, ermöglicht autorisierten Registratoren das Genehmigen oder Zurückweisen von Registrierungsanforderungen sowie das Verwalten von Zertifikaten nach deren Ausstellung.
 - Ein Prüfsubsystem berechnet einen Nachrichtenauthentifizierungscode (Message Authentication Code, MAC) für jeden Protokolleintrag. Wenn Prüfdaten nach ihrer Aufzeichnung in der Prüfdatenbank geändert oder gelöscht werden, können Sie diese Manipulation mit Hilfe des MAC feststellen.
 - Regel-Exits ermöglichen Anwendungsentwicklern die Anpassung der Registrierungsprozesse.
 - Integrierte Unterstützung für eine Steuerkomponente zur Verschlüsselung. Zur Authentifizierung der Kommunikation werden die Tivoli PKI-Hauptkomponenten mit einem werkseitig generierten privaten Schlüssel unterzeichnet. Sicherheitsobjekte wie beispielsweise Schlüssel und MACs werden verschlüsselt und in geschützten Bereichen, den sogenannten KeyStores (Schlüsselspeichern), gespeichert.
 - Integrierte Unterstützung für IBM Directory. Das Directory speichert Informationen zu gültigen und widerrufenen Zertifikaten in einem LDAP-kompatiblen Format.
 - Integrierte Unterstützung für IBM WebSphere™ Application Server und IBM HTTP Server. Der Webserver arbeitet mit dem RA-Server zusammen, um Nachrichten zu verschlüsseln, Anforderungen zu authentifizieren und Zertifikate an den vorgesehenen Empfänger zu übertragen.
 - Integrierte Unterstützung für IBM DB2® Universal Database.

Übersicht

Wenn in Ihrem Unternehmen gesicherte Anwendungen eingesetzt werden, die mit Tivoli PKI geschützt werden, können nur Benutzer, die über die entsprechenden Identitätsnachweise verfügen, auf diese Anwendungen zugreifen. Ihre gesicherten Ressourcen sowie die Unternehmensregeln zur Erteilung von Identitätsnachweisen für den Zugriff auf diese Ressourcen werden als Registrierungsdomäne bezeichnet. Die Tivoli PKI-Registrierungsfunktion stellt die Dateien und Prozesse bereit, die zur Unterstützung der Registrierungsdomäne erforderlich sind. Hierdurch können Sie die erteilten Zertifikatstypen sowie die Regeln für den Zugriff auf Ihre Anwendungen anpassen und steuern. Die Registrierungsfunktion umfasst Registrierungs- und Zertifizierungsfunktionen, eine gesicherte Datenbank und eine Verwaltungsschnittstelle.

Eine Person, die ein digitales Zertifikat benötigt, kann dieses anfordern und die hierzu benötigten Informationen auf Registrierungs-Web-Seiten angeben. Die Daten in der Registrierungsanforderung bilden die Basis für die Entscheidung darüber, ob die Anforderung genehmigt oder zurückgewiesen wird.

Die Bewertung von Registrierungsanforderungen und die Verwaltung der zugehörigen Datensätze sind Verwaltungs-Tasks. In bestimmten Fällen wird Tivoli PKI innerhalb eines Unternehmens so konfiguriert, dass Teile dieser Tasks automatisch ausgeführt und die Registrierungsdaten von einem Programm bewertet werden. In anderen Fällen werden alle Entscheidungen von einem Registrator getroffen.

Die RA von Tivoli PKI verarbeitet alle Anforderungen. Wird eine Anforderung genehmigt, stellt der CA von Tivoli PKI ein Zertifikat aus. Sowohl die Registrierungsanforderungen als auch die Zertifikate werden in einer verschlüsselten Datenbank gespeichert.

Die Tivoli PKI-Registrierungsfunktion für Ihre Registrierungsdomäne verfügt über die im Folgenden aufgeführten Funktionen und Elemente. Einige dieser Komponenten können angepasst werden:

Registrierung

Diese Softwarekomponente umfasst Registrierungs-Web-Seiten, auf denen Antragsteller Zertifikate anfordern und später über ihren Web-Browser empfangen können. Sie können eigene Unternehmensregeln für den Registrierungsprozess anwenden und hierbei auch die Funktionsweise der Web-Seiten und die Rückmeldungen an Benutzer zum Status ihrer Anforderungen anpassen.

Genehmigungsverarbeitung

Der Genehmigungsprozess unterstützt die Registrierung und Zertifizierung. Er umfasst einen Regel-Exit, der zum Automatisieren der Registrierung oder zum Anwenden Ihrer Unternehmensregeln bei der Registrierung und Zertifizierung eingesetzt werden kann. Sie können einen Regel-Exit auch zur Bereitstellung von Informationen für eine Ihrer eigenen Anwendungen benutzen.

Registrierungsstelle

Der RA-Server arbeitet bei der Registrierungsverarbeitung interaktiv mit der Registrierungsfunktion und dem CA-Server zusammen.

Zertifikatsaussteller

Der CA-Server arbeitet mit dem RA-Server zusammen und führt die Zertifizierungsverarbeitung durch.

Zertifikatsprofile

Tivoli PKI stellt Zertifikatsprofile für eine Vielzahl von Einsatzbereichen zur Verfügung. Sie können diese Profile anpassen und außerdem auf der Basis der bereitgestellten Profile weitere Profile erstellen.

Directory

Das von Tivoli PKI unterstützte Directory verwendet das LDAP-Protokoll.

Registrierungsdatenbank

Datensätze zu Registrierungsanforderungen und Zertifikaten sind in einer verschlüsselten Registrierungsdatenbank gespeichert.

Verwaltungsschnittstelle

Berechtigte Registratoren verwenden RA Desktop zum Auswerten von Registrierungsanforderungen sowie zum Verwalten von Anforderungen und Zertifikaten.

Schlüsselsicherung und -wiederherstellung

Ermöglicht die Sicherung und Wiederherstellung von Zertifikatsschlüsseln und privaten Schlüsseln in bzw. aus PKCS #12-Dateien, die von Endbenutzern erstellt wurden. Der Wiederherstellungsprozess wird über RA Desktop verwaltet.

Da zahlreiche Elemente der Registrierungsdomäne angepasst werden können, kann diese optimal auf Ihre Unternehmensschwerpunkte abgestimmt werden:

- Ihre Unternehmensregeln können die Ausführung von Registrierungs-, Zertifizierungs- und Verwaltungsoperationen bestimmen.
- Die Registrierungs-Web-Seiten können optisch an andere Dokumente und Anwendungen Ihres Unternehmens angepasst werden.
- Sie können Zertifikate anbieten, die bestimmten Anforderungen Ihrer Mitarbeiter und Kunden entsprechen.

3

Informationen zur Vorgehensweise

Die Themen in diesem Kapitel enthalten schrittweise Anweisungen zur Ausführung von Tasks, die Sie bei der Anpassung Ihrer Registrierungsdomäne ausführen müssen. Hierzu gehören z. B. folgende Operationen:

- Ändern der Darstellung der Registrierungsseiten
- Durchführen von Änderungen an einem Zertifikatsprofil

Planen der Anpassung

Gehen Sie wie folgt vor, um die Anpassung Ihres Systems zu planen:

1. Stellen Sie eine Liste der Anforderungen Ihres Unternehmens zusammen. Diese sollte z. B. folgende Informationen enthalten:
 - Welche Funktionen sollen für Zertifikate bereitgestellt werden?
 - Welche Terminologie eignet sich am besten für Ihre Benutzer, wenn diese auf die Registrierungswebseiten zugreifen?
 - Welche Anzeige soll aufgerufen werden, wenn Benutzer die Registrierungs-Web-Seite verlassen?
 - Welche Informationen soll ein Antragsteller in einer E-Mail-Benachrichtigung erhalten, nachdem eine Registrierungsanforderung verarbeitet wurde?
 - Welche Daten sollen während der Registrierung und Zertifizierung erfasst werden?
 - Welche anderen Verarbeitungsoperationen sollen während der Registrierung ausgeführt werden?
 - Welche anderen Anwendungen sollen während der Registrierung ausgeführt werden?

Beim Zusammenstellen der Liste finden Sie möglicherweise nützliche Informationen unter dem Thema "Anpassung" im Abschnitt „Erläuterungen“ auf Seite 19.

2. Ordnen Sie Ihre Anforderungen den anpassbaren Elementen bei der Registrierung und dem entsprechenden Regel-Exit sowie den zugehörigen Positionen zu.
3. Bestimmen Sie die Auswirkungen der geplanten Anpassung. Möglicherweise müssen Sie Tivoli PKI erneut starten.
4. Erstellen Sie nach der Installation Sicherungskopien aller Dateien, die geändert werden sollen.
5. Führen Sie die Änderungen entweder direkt durch oder verwenden Sie die vorhandenen anpassbaren Elemente als Schablonen zum Erstellen neuer Registrierungselemente oder Regel-Exits.

Mit Hilfe Ihrer Änderungen können Sie eine angepasste Registrierungsanwendung für Ihre Registrierungsdomäne erstellen. „Anpassungsbeispiel“ auf Seite 69, enthält ein Beispiel für eine angepasste Registrierungsanwendung, die durch entsprechende Modifikationen erstellt wurde.

Editieren anpassbarer Dateien

Bei der Durchführung von Änderungen an den Dateien, die für die Registrierungsdomäne angepasst werden sollen, müssen Sie äußerst vorsichtig vorgehen. Vor dem Ändern einer Datei sollten Sie eine Sicherungskopie erstellen. Die Verfügbarkeit einer Sicherungskopie ist besonders wichtig bei Java Server Page (JSP)-Dateien, der Konfigurationsdatei 'raconfig.cfg' sowie bei den Zertifikatsprofildateien.

Wird die Anwendung nicht in der englischen Version ausgeführt, müssen Sie außerdem einen Unicode-Editor verwenden, mit dem Daten in der nativen Codepage (z. B. im UTF-8-Format) gespeichert werden können. Unter Windows NT eignen sich die Microsoft-Editoren Notepad und Wordpad nicht zur Durchführung von Änderungen. Wenn Sie z. B. mit Microsoft Wordpad eine Datei in traditionellem Chinesisch speichern wollen, überschreibt dieser Editor bestimmte Zeichen und speichert die Daten im Big5-Format. Dies gilt auch dann, wenn die ursprüngliche Datei im UTF-8-Format codiert ist.

Informationen zu Editoren, die das Speichern von Daten in der nativen Codepage unterstützen, finden Sie in „Anpassungs-Tools“ auf Seite 41.

Anmerkung: Wenn Sie Tivoli PKI unter Windows NT installiert haben, müssen Sie allen für die Registrierungsfunktion erstellten Ressourcendateien (z. B. allen HTML- und JSP-Dateien) Namen in Kleinbuchstaben zuordnen. Der IBM HTTP-Server gibt die Fehlermeldung 'ERROR 404 NOT FOUND' aus, wenn er Dateinamen feststellt, die in Großbuchstaben oder in Groß-/Kleinschreibung angegeben sind. Verwenden Sie als Dateinamen z. B. 'my.html', jedoch nicht 'MY.html' oder 'My.html'. Dieses Problem auf dem IBM HTTP-Server betrifft Installationen von Tivoli PKI unter AIX nicht.

Anpassen der Registrierung

Sie können die Registrierungsfunktion anpassen. Durch die vorgenommenen Änderungen können die Registrierungsanforderungen Ihres Unternehmens besser unterstützt werden. Darüber hinaus können Sie die Registrierungsfunktion so anpassen, dass sie sich an den Normen und Richtlinien orientiert, die innerhalb Ihres Unternehmens für die Gestaltung von Webseiten gelten.

Directory-Einträge während der Registrierung erstellen

Im Rahmen der Erstellung von Directory-Einträgen während der Registrierung müssen Sie den folgenden Parameter in der Datei 'raconfig.cfg' angeben:

```
ldap_autoCreate_entries=false // this variable is boolean true or false
```

Das Geschäftsprozessobjekt 'LDAPCreateEntries' verfügt über zwei Betriebsarten:

- Wurde für den Parameter 'ldap_autoCreate_entries=' der Wert 'false' definiert, führt das Geschäftsprozessobjekt 'LDAPCreateEntries' keine Verarbeitungsoperation durch und im Directory werden keine Einträge erstellt. Dies ist die Standardbetriebsart.

- Wurde für den Parameter 'ldap_autoCreate_entries=' der Wert 'true' definiert, ruft das Geschäftsprozessobjekt 'LDAPCreateEntries' den Service 'LDAPPolicy' auf.
- Wenn Sie für das Argument 'PolicyClass=' keinen Wert angeben, wird die Anwendung keiner Regel erzwungen und im Directory wird automatisch ein Eintrag erstellt.

Hinzufügen eines Registrierungsfelds

Wenn Sie eine benutzerdefinierte Erweiterung zu einem der Zertifikatsprofile hinzufügen wollen, können Sie ein Feld zum Registrierungsformular hinzufügen, um diese Erweiterung zu berücksichtigen. Gehen Sie hierzu wie folgt vor:

1. Erstellen Sie eine Sicherungskopie der JSP-Datei, die das zu ändernde Registrierungsformular enthält.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die Position, an der das neue Feld eingefügt werden soll. Das neue Feld sollte zwischen dem Textfenster des vorherigen Feldes und dem beschreibenden Text für das nachfolgende Feld eingefügt werden.
4. Fügen Sie die Definition für das neue Feld ein. (Im Folgenden ist ein Beispiel aufgeführt.)
5. Speichern und schließen Sie die Datei.
6. Falls Sie diesen Arbeitsschritt nicht bereits ausgeführt haben, fügen Sie die gewünschte benutzerdefinierte Erweiterung zu einem der angebotenen Zertifikatsprofile hinzu oder erstellen Sie eine neue Profildefinition und fügen Sie die Erweiterung hinzu.

Das folgende Beispiel zeigt das Hinzufügen eines Feldes für die Telefonnummer (Telephone Number) zwischen den Feldern für den zweiten Vornamen (Second Name) und die E-Mail-Adresse (E-Mail Address).

```
<% // The second name field %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#BBE2EC">
<FONT SIZE="2">
<%= secondFieldHelp %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#9FD5E3">
<FONT SIZE="2">
<%= secondFieldLbl %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= secondFieldName %>"
onFocus="oldName=this.value;"
onChange="CreateDefaultCN( this.value );"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="<%= secondFieldMaxLength %>"
VALUE="<%= secondFieldReturnValue %>"
</TD>
</TR>

<% // Telephone Number %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#BBE2EC">
<FONT SIZE="2">
please enter your telephone number.
</FONT>
</TD>
```

```

<TD ALIGN="LEFT" BGCOLOR="#9FD5E3">
<FONT SIZE="2">
<STRONG>
Telephone Number:
</STRONG>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="phone_number" SIZE="16" MAXLENGTH="16" VALUE="">
</TD>
</TR>
<% // E-mail Address %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#BBE2EC">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[3] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#9FD5E3">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[3] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLb1 %>
<%= errorFlags[3] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[3] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="128"
VALUE="<%= inputFieldReturnValues[3] %>"
</TD>
</TR>

```

Hinzufügen eines Werts zu einer Auswahlliste

Sie können einen Wert, z. B. einen Zertifikatstyp, zu einer Auswahlliste hinzufügen, die dem Benutzer auf einer Registrierungs-Web-Seite angezeigt wird.

Gehen Sie wie folgt vor, um einen Wert hinzuzufügen:

1. Erstellen Sie eine Sicherungskopie der Datei 'raconfig.cfg'.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Zum Hinzufügen zweier neuer Profile zum Zertifikatsregistrierungsformular des Browsers Netscape müssen Sie die im Folgenden hervorgehoben dargestellten Änderungen vornehmen:

```

CertProfiles_NSBrowserSSLCert=SSLBrowserCert1Year,SSLBrowserCert2Year,
S/MIMECert1Year,S/MIMECert2Year,NewProfile1Year,NewProfile2Year

```

4. Zum Hinzufügen eines einzelnen neuen Profils zum Zertifikatsregistrierungsformular des Browsers Internet Explorer müssen Sie die im Folgenden hervorgehoben dargestellten Änderungen vornehmen:

```

CertProfiles_IEBrowserSSLCert=SSLBrowserCert1Year,SSLBrowserCert2Year,
S/MIMECert1Year,S/MIMECert2Year,NewProfile1Year

```

5. Zum Hinzufügen eines einzelnen neuen Profils zum Registrierungsformular für Server und Einheiten müssen Sie die im Folgenden hervorgehoben dargestellten Änderungen vornehmen:

```

CertProfiles_PKCS107Cert=SSLServerCert1Year,SSLServerCert2Year,
IPSecCert1Year,IPSecCert2Year,NewProfile1Year

```

6. Zum Hinzufügen eines einzelnen neuen Profils zum Registrierungsformular für die Zertifikatsvorabregistrierung und zur Anzeige dieses Profils nach 'IPSecCert2Year' müssen Sie die im Folgenden hervorgehoben dargestellten Änderungen vornehmen:

```
CertProfiles_PreReg=S/MIMECert1Year,S/MIMECert2Year,IPSecCert1Year,IPSecCert2Year,
NewProfile1Year,SSLServerCert1Year,SSLServerCert2Year,SSLBrowserCert1Year,
SSLBrowserCert2Year,SignatureOnlyCert1Year,SignatureOnlyCert2Year,
KeyEnciphermentCert1Year,KeyEnciphermentCert2Year,DataEnciphermentCert1Year,
DataEnciphermentCert2Year,NonRepudiationCert1Year,NonRepudiationCert2Year,
CACrossCertificationRequest
```

7. Speichern und schließen Sie die Datei.

Anmerkung: Die neuen Profile müssen in der Datei 'certificate_profiles.cfg' vordefiniert werden.

Ändern von Bildmaterial auf einer Registrierungsseite

Gehen Sie wie folgt vor, um Bildmaterial zu einer Registrierungsseite hinzuzufügen:

1. Speichern Sie das gewünschte Bildmaterial in einer GIF-Datei (.gif).
2. Erstellen Sie für die zu ändernde Registrierungsseite eine Sicherungskopie der JSP-Datei.
3. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
4. Suchen Sie die Formatierungssteuerzeichen für das Bildmaterial, das ersetzt werden soll. Sie haben voraussichtlich folgendes Format:

```
IMG SRC="<%= UE_SERVER_AUTH_URL_PATH %><%= JSP_MOUNT_POINT %>SW_Banner.gif"
WIDTH="600" HEIGHT="27" BORDER="0" ALT="IBM SecureWay">
```

5. Setzen Sie, wie im Folgenden hervorgehoben dargestellt, den Namen Ihrer GIF-Datei ein:

```
IMG SRC="<%= UE_SERVER_AUTH_URL_PATH %><%= JSP_MOUNT_POINT %>MyBanner.gif"
WIDTH="600" HEIGHT="27" BORDER="0" ALT="IBM SecureWay">
```

Ändern von Text auf einer Registrierungsseite

Gehen Sie wie folgt vor, um den Text auf einer Registrierungsseite zu ändern:

1. Erstellen Sie für die zu ändernde Registrierungsseite eine Sicherungskopie der JSP-Datei.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Führen Sie am Text und an den Formatierungssteuerzeichen die erforderlichen Änderungen durch.
4. Speichern und schließen Sie die Datei.

Ändern von Text im Benachrichtigungsbrief

Im Benachrichtigungsbrief werden die Antragsteller darüber informiert, dass ihre Registrierungsanforderung verarbeitet wurde. Es wird ihnen in dieser Nachricht jedoch nicht mitgeteilt, ob die Anforderung genehmigt wurde. Sie können den Text des Briefes, jedoch nicht seine Bedeutung ändern.

Gehen Sie wie folgt vor, um den Text zu ändern:

1. Erstellen Sie eine Sicherungskopie der Mail-Schablonendatei (Mail_*.ltr), die angepasst werden soll.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Führen Sie am Text und an den Formatierungssteuerzeichen die erforderlichen Änderungen durch.
4. Speichern und schließen Sie die Datei.

Herstellen einer Verbindung zur Registrierung über eine andere URL-Adresse

Gehen Sie wie folgt vor, um über eine eigene Web-Seite eine Verbindung zur Registrierungs-Web-Seite herzustellen:

1. Öffnen Sie die Quelle Ihrer Web-Seitendatei mit einem Editor, der das UTF-8-Format unterstützt.
2. Suchen Sie die Position, an der die Verbindung platziert werden soll.
3. Fügen Sie die folgende Zeile ein, wobei `<URL for index.jsp>` für die vollständig qualifizierte URL-Adresse der Seite 'index.jsp' steht:
`<A HREF="<URL for index.jsp>">Certificate Enrollment</A>`

Beispiel:

`http://myserver.mycompany.com/YourDomain/index.jsp`

4. Speichern und schließen Sie die Datei.

Aktivieren der automatischen Anforderungsverarbeitung

Die Genehmigung und Erneuerbarkeit einer Registrierungsanforderung wird durch das während der Registrierungsanforderung ausgewählte Zertifikatsprofil definiert. Standardmäßig setzt ein Zertifikatsprofil eine Anforderung automatisch in den Wartestatus (pend) und definiert diese als nicht erneuerbar (false). Um diese Prozedur zu ändern und Anforderungen z. B. automatisch zu genehmigen und automatisch als erneuerbar zu definieren, müssen Sie in der Datei 'certificate_profiles.cfg' eine oder beide der folgenden Einstellungen zur Zeilen-gruppe des Zertifikatsprofils hinzufügen.

```
; --- Auto: approve or pend
decision_default=approve

; --- renewable: true or false
credential_renewable=true
```

Aktivieren der E-Mail-Benachrichtigung unter Windows NT

Die Registrierungsfunktion des Web-Browsers ermöglicht Ihnen das Empfangen einer E-Mail-Benachrichtigung zum Status Ihrer Zertifikatsanforderungen. Um diese Funktion in einer Windows NT-Umgebung zu aktivieren, müssen Sie entweder für den RA-Server einen lokalen SMTP-Server (Simple Mail Transfer Protocol) konfigurieren oder einen Zeiger auf einen SMTP-Host in der Konfigurationsdatei der Registrierungsfunktion definieren.

Gehen Sie wie folgt vor, um einen Zeiger auf einen SMTP-Server zu definieren:

1. Editieren Sie die Datei 'raconfig.cfg'. Der Standardinstallationspfad für diese Datei lautet 'C:\Program Files\IBM\Trust Authority\pkrf\Domains\domain_name\etc\'.
2. Fügen Sie die folgende Zeile am Ende der Datei hinzu, wobei `host.domain.com` für den SMTP-Server steht:
`SMTP_HOST_NAME=host.domain.com`

Anmerkung: Bei der Durchführung von Änderungen an der Datei 'raconfig.cfg' müssen Sie äußerst vorsichtig vorgehen. Informationen zum Einsatz eines Editors, der das UTF-8-Format unterstützt, finden Sie unter „Anpassungs-Tools“ auf Seite 41. Ausführliche Informationen zur Datei 'raconfig.cfg' enthält der Abschnitt „Konfigurationsdatei für die Registrierungsfunktion“ auf Seite 51.

Anpassen des Regel-Exits

Sie können den Regel-Exit anpassen oder einen eigenen Exit hinzufügen, um zusätzliche Verarbeitungsoperationen auszuführen oder mit anderen Anwendungen Ihres Unternehmens interaktiv zusammenzuarbeiten.

Bei dem Regel-Exit kann es sich um eine beliebige ausführbare Datei, z. B. um eine C++-, Shell- oder eine andere Komponente, handeln. Der Exit dient zum Lesen von Eingabenachrichten mit Name-/Wert-Paaren (name=value) aus der Standardeingabeeinheit (STDIN). Er schreibt entsprechende Ausgabenachrichten mit Name-/Wert-Paaren in die Standardausgabeeinheit (STDOUT).

Identifizieren des Regel-Exit-Namens

Der Eintrag 'afservice.PolicyExit' in der Datei 'raconfig.cfg' identifiziert das Regel-Exit-Programm, das von einem Geschäftsprozess aufgerufen werden soll. Im folgenden Beispiel wird dieser Eintrag dargestellt, wobei *install_path* den vollständigen Pfad der ausführbaren Datei für Ihr angepasstes Regel-Exit-Programm definiert.

```
afservice.PolicyExit=com.ibm.irg.ra.afw.services.SpawnPolicyExitLongRunningFactory,
install_path\custom_program_name
```

Anmerkungen:

1. Tivoli PKI unterstützt nur einen Regel-Exit-Eintrag.
2. Wird Tivoli PKI unter Windows NT ausgeführt, müssen Sie für neue Dateinamen Kleinbuchstaben verwenden. Momentan kann der HTTP-Server Dateien, deren Namen auch Großbuchstaben enthalten, nicht lokalisieren.

Weitere Informationen zum Schreiben von Regel-Exits finden Sie in „Einschränkungen bei Regel-Exits“ auf Seite 21 und „Schnittstellen zum Regel-Exit“ auf Seite 22. Eine Liste der Beispiel-Regel-Exits enthält der Abschnitt „Regel-Exit-Datei“ auf Seite 49.

Ändern des Beispiel-Regel-Exits

Sie können den zum Lieferumfang von Tivoli PKI gehörenden Beispiel-Regel-Exit 'auto_approve' ändern oder durch einen eigenen, angepassten Exit ersetzen. Diese Exits dienen zur Ausführung bestimmter, in Ihrem Unternehmen benötigter Verarbeitungsoperationen oder zum interaktiven Zusammenarbeiten mit anderen Anwendungen Ihres Unternehmens.

Gehen Sie wie folgt vor, um den Beispiel-Regel-Exit zu ändern:

1. Erstellen Sie Sicherungskopien der vorhandenen Beispielquellendatei 'auto_approve.cpp' sowie der ausführbaren Datei 'auto_approve.exe'. Speichern Sie diese Dateien an einer sicheren Position.
2. Ändern Sie die Beispielquellendatei entsprechend Ihren individuellen Anforderungen. Beachten Sie hierbei, dass die Geschäftsprozesse, die zum Lieferumfang von Tivoli PKI gehören, Abhängigkeiten zu bestimmten Werten aufweisen, die an den Regel-Exit übergeben (z. B. decision_default) oder von diesem zurückgegeben werden (z. B. reqStatus und ffStatus). Wenn Sie die Art und Weise ändern wollen, in der diese Werte von dem gelieferten Regel-Exit verwendet werden, müssen Sie die Änderungen genau planen und sicherstellen, dass hierbei keine Benutzungskonflikte mit den Geschäftsprozessen von Tivoli PKI entstehen.
3. Nach dem Ändern und Kompilieren sollten Sie die ausführbare Datei des Regel-Exits an die selbe Position kopieren, an der die ausführbare Datei der zum Lieferumfang gehörenden Komponente gespeichert ist. Beispiel:

-
- Unter AIX: /usr/lpp/iau/pkrf/Domains/*YourDomain*/bin
 - Unter Windows NT: C:\Program Files\IBM\Trust Authority\pkrf\Domains*YourDomain*\bin
4. Solange die von den zugehörigen Beispiel-Make-Dateien erstellte ausführbare Datei nicht umbenannt wird, müssen die Einträge in der Datei 'raconfig.cfg' nicht aktualisiert werden.
 5. Stoppen Sie Tivoli PKI und führen Sie anschließend einen Neustart durch.

Weitere Informationen zum Schreiben eines Regel-Exits finden Sie in „Einschränkungen bei Regel-Exits“ auf Seite 21 und „Schnittstellen zum Regel-Exit“ auf Seite 22. Eine Liste der Beispiel-Regel-Exits enthält der Abschnitt „Regel-Exit-Datei“ auf Seite 49.

Ersetzen des Beispiel-Regel-Exits

Verwenden Sie diese Prozedur, um den zum Lieferumfang von Tivoli PKI gehörigen Beispiel-Regel-Exit 'auto_approve' zu ersetzen:

1. Erstellen Sie Sicherungskopien der vorhandenen Beispielquellendatei 'auto_approve.cpp' sowie der ausführbaren Datei 'auto_approve.exe'. Speichern Sie diese Dateien an einer sicheren Position.
2. Entwickeln Sie den angepassten Quellencode. Beachten Sie hierbei, dass die Geschäftsprozesse, die zum Lieferumfang von Tivoli PKI gehören, Abhängigkeiten zu bestimmten Werten aufweisen, die an den Regel-Exit übergeben (z. B. 'decision_default') oder von diesem zurückgegeben werden (z. B. 'reqStatus' und 'ffStatus'). Wenn Sie die Art und Weise ändern wollen, in der diese Werte von dem gelieferten Regel-Exit verwendet werden, müssen Sie die Änderungen genau planen und sicherstellen, dass hierbei keine Benutzungskonflikte mit den Geschäftsprozessen von Tivoli PKI entstehen.
3. Nach dem Ändern und Kompilieren sollten Sie die ausführbare Datei des Regel-Exits an die selbe Position kopieren, an der die ausführbare Datei der zum Lieferumfang gehörenden Komponente gespeichert ist. Beispiel:
 - Unter AIX: /usr/lpp/iau/pkrf/Domains/*YourDomain*/bin
 - Unter Windows NT: C:\Program Files\IBM\Trust Authority\pkrf\Domains*YourDomain*\bin
4. Ändern Sie den Eintrag 'afservice.PolicyExit' in der Datei 'raconfig.cfg' so, dass dieser auf die ausführbare Datei für den neuen Regel-Exit zeigt. (Ein Beispiel hierzu finden Sie in „Identifizieren des Regel-Exit-Namens“ auf Seite 11.)
5. Stoppen Sie Tivoli PKI und führen Sie anschließend einen Neustart durch.

Weitere Informationen zum Schreiben eines Regel-Exits finden Sie in „Einschränkungen bei Regel-Exits“ auf Seite 21 und „Schnittstellen zum Regel-Exit“ auf Seite 22. Eine Liste der Beispiel-Regel-Exits enthält der Abschnitt „Regel-Exit-Datei“ auf Seite 49.

Anpassen von Zertifikaten

Sie können Ihre Zertifikatsangebote anpassen. Hierzu müssen Sie entweder die vorhandenen Zertifikatsprofile ändern oder neue Profile erstellen. Darüber hinaus können Sie X.509v3-Benutzererweiterungen hinzufügen.

Zur Unterstützung Ihrer Benutzer können Sie außerdem die Anzeigenamen und die Beschreibungen vorhandener Angebote ändern.

Hinzufügen eines Zertifikatsprofils

Sie können ein Zertifikatsprofil erstellen, das eine andere Kombination aus Kenndaten enthält. Beispiel:

- Standardeinstellung für den Gültigkeitszeitraum
- Verfügbares Leistungsspektrum

Anmerkung: Vor dem Hinzufügen einer neuen Zertifikatsprofildefinition oder dem Ändern eines Profils, das durch die Standardinstallation von Tivoli PKI bereitgestellt wurde, sollten Sie sich mit den Regeln und Verarbeitungsvoraussetzungen vertraut machen, die in „Zertifikatsprofile“ auf Seite 29 erläutert werden.

Gehen Sie wie folgt vor, um ein neues Profil zu erstellen:

1. Erstellen Sie eine Sicherungskopie der Datei 'certificate_profiles.cfg' für Ihre Registrierungsdomäne.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die (durch eckige Klammern [] gekennzeichnete) Zeilengruppe, die mit der zu erstellenden Zeilengruppe identisch ist.
4. Kopieren Sie diese Zeilengruppe und fügen Sie sie in die Datei ein. Ändern Sie diese anschließend so, dass sie die gewünschten Kenndaten enthält.
5. Speichern und schließen Sie die Datei.
6. Fügen Sie eine Beschreibung des Zertifikatstyps zu den Angaben hinzu, die der Antragsteller anzeigen kann.

Hinzufügen der Beschreibung eines Zertifikatstyps

Während der Registrierung wird den Antragstellern eine Liste der verfügbaren Zertifikatstypen angezeigt. Das Registrierungsformular enthält eine Verbindung zu Beschreibungen dieser Zertifikatstypen, um dem Antragsteller die Auswahl zu erleichtern. Nach dem Hinzufügen eines neuen Zertifikatsprofils und der Zuordnung eines Anzeigenamens können Sie dessen Beschreibung zu den anderen Beschreibungen hinzufügen. Gehen Sie hierzu wie folgt vor:

1. Erstellen Sie eine Sicherungskopie von 'CertTypes.jsp'. Diese Datei enthält eine Beschreibung der Zertifikatstypen, die die Antragsteller anzeigen und auswählen können.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die Position, an der der neue Zertifikatstyp beschrieben werden soll.
4. Kopieren Sie den Text einer ähnlichen Zertifikatstypbeschreibung und fügen Sie diesen ein.
5. Ändern Sie den Text entsprechend Ihren individuellen Anforderungen.
6. Speichern und schließen Sie die Datei.

Ändern eines Zertifikatsprofils

Sie können bestimmte Kenndaten eines Zertifikatsprofils ändern. Hierzu gehören z. B. die folgenden Komponenten:

- Standardeinstellung für den Gültigkeitszeitraum
- Wichtigste Verwendungsbereiche für den Zertifikatstyp

Anmerkung: Vor dem Ändern einer vorhandenen Profildefinition sollten Sie sich mit den Regeln und Verarbeitungsvoraussetzungen vertraut machen, die in „Zertifikatsprofile“ auf Seite 29 erläutert sind.

Gehen Sie wie folgt vor, um ein Profil zu ändern:

1. Erstellen Sie eine Sicherungskopie der Datei 'certificate_profiles.cfg' für Ihre Registrierungsdomäne.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die (durch eckige Klammern [] gekennzeichnete) Zeilengruppe, die der zu ändernden Zeilengruppe entspricht.
4. Modifizieren Sie die Zeilen, die die gewünschten Änderungen (z. B. die Standardeinstellung für den Gültigkeitszeitraum) steuern.
5. Speichern und schließen Sie die Datei.
6. Ändern Sie die Beschreibung des Zertifikatstyps so, dass diese die am Profil durchgeführten Änderungen wiedergibt.

Ändern der Beschreibung eines Zertifikatstyps

Während der Registrierung wird den Antragstellern eine Liste der verfügbaren Zertifikatstypen angezeigt. Das Registrierungsformular enthält eine Verbindung zu Beschreibungen dieser Zertifikatstypen, um dem Antragsteller die Auswahl zu erleichtern.

Gehen Sie wie folgt vor, um die Beschreibung eines Zertifikatstyps zu ändern:

1. Erstellen Sie eine Sicherungskopie von 'CertTypes.jsp'. Diese Datei enthält eine Beschreibung der Zertifikatstypen.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die Zeilen, die die zu ändernde Beschreibung enthalten.
4. Ändern Sie den Text entsprechend Ihren individuellen Anforderungen.
5. Speichern und schließen Sie die Datei.

Ändern des Anzeigenamens eines Zertifikatstyps

Gehen Sie wie folgt vor, um die Namen der Zertifikatstypen zu ändern, die Benutzer auf dem Registrierungsformular anzeigen und auswählen können:

1. Erstellen Sie eine Sicherungskopie der Datei 'certificate_profiles.cfg' für Ihre Registrierungsdomäne.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die (durch eckige Klammern [] gekennzeichnete) Zeilengruppe, die den umzubenennenden Zertifikatstyp definiert.

4. Suchen Sie die Zeile 'display_name' und ändern Sie diese entsprechend Ihren individuellen Anforderungen. Das folgende Beispiel zeigt die Originaldefinition und eine mögliche Änderung:

```
; --- S / M I M E C e r t 1 Y e a r ---  
[S/MIMECert1Year] display_name=E-mail Protection (1-Year)  
required_fields=first_name,last_name,email_address  
; --- S / M I M E C e r t 1 Y e a r ---  
[S/MIMECert1Year] display_name=Secure E-mail (1-Year)  
required_fields=first_name,last_name,email_address
```

5. Speichern und schließen Sie die Datei.

Löschen eines Zertifikatsprofils

Gehen Sie wie folgt vor, um ein Zertifikatsprofil zu löschen, wenn Sie den Antragstellern den zugehörigen Zertifikatstyp nicht zur Verfügung stellen wollen:

Anmerkung: Vor dem Löschen einer vorhandenen Zertifikatsprofildefinition sollten Sie sich mit den Regeln und Verarbeitungsvoraussetzungen vertraut machen, die in „Zertifikatsprofile“ auf Seite 29 erläutert sind.

1. Erstellen Sie eine Sicherungskopie der Datei 'certificate_profiles.cfg' für Ihre Registrierungsdomäne.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die (durch eckige Klammern [] gekennzeichnete) Zeilengruppe, die dem zu löschenden Profil entspricht. Globale Profilwerte dürfen nicht gelöscht werden.
4. Verwenden Sie ein Semikolon (;), um die gesamte Zeilengruppe auf Kommentar zu setzen.
5. Speichern und schließen Sie die Datei.
6. Löschen Sie die Beschreibung des Zertifikatstyps, so dass die Antragsteller die zugehörige Beschreibung nicht anzeigen können.

Löschen der Beschreibung eines Zertifikatstyps

Gehen Sie wie folgt vor, um die Beschreibung eines Zertifikatstyps aus dem Text zu löschen, dem Antragsteller weiterführende Informationen entnehmen können:

1. Erstellen Sie eine Sicherungskopie von 'CertTypes.jsp'. Diese Datei enthält eine Beschreibung der Zertifikatstypen.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die Zeilen, die die zu löschende Beschreibung enthalten.
4. Verwenden Sie ein Semikolon (;), um den Text auf Kommentar zu setzen.
5. Speichern und schließen Sie die Datei.

Hinzufügen von Benutzererweiterungen zu einem Zertifikatsprofil

Gehen Sie wie folgt vor, um benutzerdefinierte Erweiterungen zu einem Zertifikatsprofil hinzuzufügen:

1. Erstellen Sie eine Sicherungskopie der Datei 'certificate_profiles.cfg' für Ihre Registrierungsdomäne.
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die (durch eckige Klammern [] gekennzeichnete) Zeilengruppe, die das zu ändernde Profil definiert.
4. Fügen Sie die gewünschten benutzerdefinierten Erweiterungen ein.
5. Speichern und schließen Sie die Datei.

Ändern der angezeigten URL-Adresse nach Verlassen von RA Desktop

Gehen Sie wie folgt vor, um die Web-Seite zu ändern, die Registratoren angezeigt wird, wenn sie RA Desktop verlassen:

1. Erstellen Sie eine Sicherungskopie von 'radesktop.jsp'. Diese Datei dient zum Anpassen von RA Desktop. Der Standardinstallationspfad für diese Datei lautet folgendermaßen:
 - Unter AIX: /usr/lpp/iau/Domains/*YourDomain*/webpages
 - Unter Windows NT: C:\Program Files\IBM\Trust Authority\Domains*YourDomain*\webpages
2. Öffnen Sie die Datei mit einem Editor, der das UTF-8-Format unterstützt.
3. Suchen Sie die Zeile, die die Zeichenfolge **exit_url** enthält.
4. Editieren Sie die Zeile und stellen Sie sicher, dass der Wert des Parameters 'exit_url' auf die Webadresse zeigt, die nach dem Verlassen von RA Desktop aufgerufen werden soll. Beispiel:

```
<PARAM NAME="exit_url" VALUE="http://userdefined-url...">
```

Hierbei ist *userdefined-url* die Webadresse.

5. Speichern und schließen Sie die Datei.

Anpassen der Sicherung und Wiederherstellung von Schlüsseln

Sie können die Funktion für die Sicherung und Wiederherstellung von Schlüsseln anpassen, indem Sie die Funktion zunächst inaktivieren und anschließend die Anforderungsinformationen ändern oder die Funktion zum automatischen Genehmigen von Wiederherstellungsanforderungen aktivieren.

Anmerkung: Die Datenbank 'krbdb' für Sicherungen/Wiederherstellungen sollte stets mit Hilfe der vorhandenen DB2-Sicherungsprozeduren gesichert werden.

Inaktivieren der Sicherung und Wiederherstellung von Schlüsseln

Führen Sie mindestens einen der folgenden Schritte aus, um die Sicherung und Wiederherstellung von Schlüsseln zu inaktivieren:

1. Entfernen Sie vor dem Starten von Tivoli PKI die zugeordneten JSP-Seiten aus der Datei 'raconfig.cfg'.
2. Entfernen Sie vor dem Starten von Tivoli PKI die zugeordneten Geschäftsprozesse aus der Datei 'BPTemplates.cfg'.
3. Entfernen Sie nach der Installation die zugeordneten JSP-Seiten.
4. Entfernen Sie den Knopf **Zur Schlüsselsicherungsanforderung** von den 'JSP-Seiten für die Genehmigung'.
5. Entfernen Sie den Eintrag **Kennwort der PKCS #12-Datei** von der JSP-Seite der **Schlüsselsicherungsanforderung**.

Ändern der Anforderungsinformationen

Führen Sie die folgenden Schritte aus, um ein Anforderungsfeld zu ändern:

1. Erstellen Sie eine Sicherungskopie der zu ändernden JSP-Datei.
2. Suchen Sie die Position des zu ändernden Felds.
3. Ändern Sie das Feld entsprechend Ihren individuellen Anforderungen.
4. Speichern und schließen Sie die Datei.

Anmerkung: Beim Entfernen des Felds **Kennwort der PKCS #12-Datei** aus der JSP-Datei für die **Schlüsselsicherungsanforderung** wird die Schlüsselsicherungsfunktion inaktiviert, da das eingegebene Kennwort zur Überprüfung der eingegebenen PKCS #12-Datei verwendet wird. Kann die Gültigkeit einer PKCS #12-Datei nicht geprüft werden, schlägt die Schlüsselsicherung für diese Datei fehl.

Aktivieren der automatischen Genehmigung

Sie haben die Möglichkeit, die automatische Genehmigung von Schlüsselwiederherstellungsanforderungen zu aktivieren. Werden die Schlüsselwiederherstellungsanforderungen automatisch genehmigt, braucht der RA-Administrator die einzelnen Schlüsselwiederherstellungsanforderungen nicht mehr über RA Desktop zu prüfen und zu genehmigen.

Führen Sie die folgenden Schritte aus, um die automatische Genehmigung von Schlüsselwiederherstellungsanforderungen zu aktivieren:

1. Erstellen Sie eine Sicherungskopie der Datei 'BPTemplates.txt'.
2. Öffnen Sie die Datei mit einem Texteditor, der das UTF-8-Format unterstützt.
3. Suchen Sie den Geschäftsprozess 'KeyRecoveryRequest'.
4. Suchen Sie die folgende Zeile im Geschäftsprozess 'KeyRecoveryRequest':
`simplebean ( SetKBPending, com.ibm.irg.ra.efw.bpos.SetKRRequestStatus,"Pending" );`
5. Editieren Sie die Zeile wie folgt:
`simplebean ( SetKBPending, com.ibm.irg.ra.efw.bpos.SetKRRequestStatus,"Approved" );`
6. Speichern und schließen Sie die Datei.

4

Erläuterungen

Dieser Abschnitt beschreibt, wie die Komponenten von Tivoli PKI zusammenarbeiten, um alle Funktionen Ihrer Registrierungsfunktion zu unterstützen. Die Themen definieren und beschreiben Konzepte, die mit der Registrierung, Zertifizierung und Verwaltung in Zusammenhang stehen und Sie beim Anpassen Ihrer Registrierungsfunktion unterstützen.

Anpassung

Der vorliegende Abschnitt enthält Hinweise, die Ihnen die zeitliche Planung von Anpassungs-Tasks erleichtern, die in einer Abhängigkeitsbeziehung zueinander stehen.

Anpassbare Elemente

Die folgenden Anwendungskomponenten können angepasst werden:

- Registrierungs-Web-Seiten, auf denen Benutzer Zertifikate anfordern können
- E-Mail-Benachrichtigungen zur Information des Benutzers nach der Verarbeitung seiner Anforderung
- Typen und Funktionen der angebotenen Zertifikate
- Regel-Exit zur Implementierung eigener Unternehmensregeln bei der Registrierung und Zertifizierung

Änderungen, die einen Systemwiederanlauf erfordern

Bestimmte Anpassungs-Tasks werden erst nach einem Wiederanlauf des Systems wirksam. Werden diese Änderungen nach dem Starten von Tivoli PKI ausgeführt, muss das System anschließend heruntergefahren und dann erneut gestartet werden, um sie zu aktivieren. Ermitteln Sie in enger Abstimmung mit Ihrem Systemadministrator einen geeigneten Zeitpunkt für das Wiederanlaufverfahren, insbesondere dann, wenn eine neue Unternehmensregel für die Registrierungs- und Zertifizierungsverarbeitung angewandt wird.

Registrierung

Bei der Registrierung wird ein Antrag auf Erteilung eines Zertifikats gestellt. In Tivoli PKI füllen die Benutzer hierfür ein Tivoli PKI-Registrierungsformular aus und übergeben dieses über ihren Webbrowser. Bei Tivoli PKI-Standardinstallationen befinden sich die Registrierungsformulare auf einer Webseite namens "Identitätsnachweis - Verwaltung".

Die Daten der Registrierungsformulare werden in Datenbanksätzen gespeichert, die ein Registrator über RA Desktop anzeigen kann.

Im Rahmen der Anpassung kann Ihr Unternehmen dieser Seite einen anderen Namen zuordnen oder Änderungen an ihr vornehmen, um sie besser auf die Darstellung der unternehmensinternen Dokumente abzustimmen. Weitere Informationen zur von der Standardinstallation unterstützten Registrierung finden Sie im *Tivoli PKI Benutzerhandbuch*.

Registrierungsfunktion

Die Registrierungsfunktion ist eine Komponente der Registrierungsfunktion von Tivoli PKI. Sie umfasst die Registrierungs-Web-Seiten und die zugehörigen Verarbeitungsfunktionen. Die Registrierungsfunktion verfügt über Schnittstellen zu den Webbrowsern der Antragsteller sowie zum Regel-Exit. Sie können die Registrierungsfunktion anpassen und hierbei folgende Komponenten ändern:

- Elemente der Web-Seiten, die eine Front-End-Komponente für die Registrierungsfunktion bereitstellen
- Text des E-Mail-Benachrichtigungsbriefes an die Antragsteller

Die Änderungen ermöglichen Ihnen die Anwendung Ihrer Unternehmensregeln auf die Durchführung des Registrierungsprozesses.

Registrierungswebseiten

Sie können die Registrierungswebseiten von Tivoli PKI zum Anfordern von Zertifikaten verwenden. Auf diese Seiten kann über den Webbrowser unter einer Webadresse auf Ihrem öffentlichen Webserver zugegriffen werden. Der Standardname für diese Web-Seiten lautet 'Identitätsnachweis - Verwaltung'. Bei Ihrem ersten Besuch der Webseite laden Sie ein CA-Zertifikat herunter, damit die Registrierungsfunktion Ihren Browser authentifizieren kann. Nach dem Erhalt dieses Zertifikats führen Sie die folgenden Arbeitsschritte aus:

1. Wählen Sie den Registrierungstyp aus, den Sie anfordern wollen:

- Browser-Registrierung
- Server- oder Einheitenregistrierung
- Zertifikatsvorabregistrierung

Diese Auswahl steuert die Felder auf Ihrem Registrierungsformular sowie den Zertifikatstyp, den Sie in der Anforderung angeben können.

2. Füllen Sie das angezeigte Formular aus und übergeben Sie es.

3. Kehren Sie später auf die Registrierungswebseiten zurück, um festzustellen, ob Ihre Anforderung genehmigt wurde. Ist dies der Fall, werden Ihnen die entsprechenden Dateien zugesendet.

- Wenn Sie ein Browserzertifikat empfangen, wird es auf Ihren Browser heruntergeladen.
- Wenn Sie ein Server- oder Einheitenzertifikat empfangen, wird dieses für die weitere Übertragung an den Server bzw. die Einheit für Sie heruntergeladen.
- Für die Vorabregistrierung von Zertifikaten empfangen Sie bestimmte Daten oder können auswählen, welcher Dateityp heruntergeladen werden soll.

Wenn Sie über diese Webseiten ein Browserzertifikat erhalten haben, können Sie diese Seiten erneut aufrufen, um Ihr Zertifikat zu erneuern oder zu widerrufen.

Vorabregistrierung

Tivoli PKI ermöglicht einem Programm oder einem Administrator die Vorabregistrierung zukünftiger Benutzer. Die für die Vorabregistrierung erforderlichen Informationen können vom zukünftigen Benutzer oder aus den Datenbeständen des zugehörigen Unternehmens (z. B. aus einer Datenbank) stammen. Nach dem Erfassen der Informationen greift der Administrator über einen Web-Browser auf die Registrierungsseite zu. Mit Hilfe eines speziellen Registrierungsformulars für die Vorabregistrierung stellt der Administrator die Registrierungsinformationen bereit und fordert Zertifikate an.

Wenn die Anforderung genehmigt wird, erhält der Administrator bestimmte Informationen, die an den zukünftigen Zertifikatseigner weitergeleitet werden müssen. Diese Person kann das Zertifikat dann mit einer PKIX-kompatiblen Anwendung herunterladen.

Weitere Informationen zur Vorabregistrierung finden Sie im *Tivoli PKI Benutzerhandbuch*.

Webbrowserunterstützung

Tivoli PKI ermöglicht es Benutzern, eine Registrierungsanforderung zu erstellen, indem Sie über einen der folgenden Web-Browser ein Registrierungsformular ausfüllen und übergeben:

- Microsoft Internet Explorer, ab Release 5.0.
- Netscape Navigator oder Netscape Communicator, ab Version 4.7.

Beim Browser für RA Desktop sind neuere Versionen dieser Browser erforderlich.

Regel-Exits

Sie können den zum Lieferumfang von Tivoli PKI gehörenden Beispiel-Regel-Exit 'auto_approve' ändern oder durch einen anderen Exit ersetzen. Darüber hinaus können Sie eigene Regel-Exit-Programme schreiben.

Einschränkungen bei Regel-Exits

Auf Grund der Art und Weise, in der Tivoli PKI-Geschäftsprozesse Regel-Exit-Programme aufrufen und mit diesen kommunizieren, müssen die Ein- und Ausgabenachrichten von Regel-Exits ein spezifisches Format aufweisen. Dieses Format besteht aus Gruppen von Name/Wert-Paaren (name=value), die in Übereinstimmung mit den URL-Standardcodierungsregeln formatiert sind. (Dieses Format ähnelt dem Format von Daten, die an CGI-Funktionen gesendet werden, wenn Sie mit der POST-Methode für das Senden von Formularen von HTML-Seiten arbeiten.)

Bei der URL-Codierung gelten die folgenden Regeln:

- Name/Wert-Paare (name=value) sind mit Et-Zeichen (&) zu begrenzen.
- Leerzeichen innerhalb eines Wertes sind durch ein Pluszeichen (+) zu ersetzen.
- Bestimmte andere Zeichen, die in einem Wert auftreten können (z. B. aus der Gruppe ~!#\$%^&()=+|\/) werden durch ein Prozentzeichen (%) ersetzt, das der hexadezimalen Entsprechung des ersetzten Zeichens vorangestellt wird.

Die Name-/Wert-Paare

```
decision_default=approve
username=John Q. Public
```

werden z. B. folgendermaßen codiert und gesendet:

```
decision_default=approve&username=John+Q.+Public
```

Beachten Sie hierbei, dass dieses Format das Verschachteln von Name-/Wert-Paaren ermöglicht. Dies bedeutet, dass der Wert des Name-/Wert-Paares wiederum andere URL-codierte Name-/Wert-Paare enthalten kann.

Um die Komplexität bei der Verwendung dieses Nachrichtenformats auf ein Minimum zu reduzieren, verwendet der Beispiel-Regel-Exit das Objekt 'raMessage'. Dieses Objekt stellt eine Reihe von Methoden zum Erstellen von Nachrichten, zum Ändern des Inhalts sowie zum Übertragen des tatsächlichen Nachrichteninhalts im geeigneten Format zur Verfügung. Hierbei ist es für den Benutzer nicht erforderlich, die exakten Details der URL-Codierung bzw. -Decodierung zu kennen.

Die zum Lieferumfang von Tivoli PKI gehörenden Geschäftsprozesse kommunizieren mit Regel-Exits über einen Service, der zum Austauschen von Nachrichten Pipes zur Standard-eingabe- (STDIN) und Standardausgabeeinheit (STDOUT) des Regel-Exit-Programms verwendet.

- Regel-Exits müssen Eingabenachrichtendaten aus der Steuereingabedatei (STDIN) lesen.
- Regel-Exits müssen die zugehörigen Antworten in die Steuerausgabedatei (STDOUT) schreiben.

Zur Gewährleistung der Konsistenz mit den gelieferten Tivoli PKI-Geschäftsprozessen müssen angepasste Regel-Exits die folgenden Rückgabedaten in Übereinstimmung mit den Aktionen definieren, die von nachfolgenden Geschäftsprozessen ausgeführt werden müssen.

Gewünschte Aktion	Vom Regel-Exit zurückzugebendes Name-/Wert-Paar
Anforderung genehmigen	reqStatus=Approved
Anforderung zurückstellen	reqStatus=Pended
Widerrufaktion ausführen	ffStatus=Revoked
Anforderung zurückweisen	reqStatus=Rejected

Schnittstellen zum Regel-Exit

Der Regel-Exit ist ein integraler Bestandteil der Registrierungsfunktion von Tivoli PKI. Er ermöglicht einem Unternehmen das Einfügen angepasster Logikelemente an verschiedenen Punkten innerhalb der Registrierungs-, Genehmigungs- und Genehmigungsnachbereitungsprozesse. Standardmäßig ruft Tivoli PKI den Beispiel-Regel-Exit z. B. während der folgenden Prozesse auf:

- Browser-SSL-Zertifikatsregistrierungsanforderungen
- Browser-SSL-Zertifikatserneuerungsanforderungen
- PKCS #10- und PKCS #7-Zertifikatsregistrierungsanforderungen
- Vom Endbenutzer eingeleitete Widerrufsanforderungen
- Vorabregistrierungsanforderungen
- Nach der Ausstellung eines Zertifikats an einen Client
- Während den von RA Desktop eingeleiteten Aktionen (Genehmigung, Zurückweisung, Zurückstellung und Widerruf)

Wenn ein Regel-Exit-Programm von der Geschäftsprozessunterstützung für die Tivoli PKI-Registrierung und RA Desktop aufgerufen wird, werden zwei wichtige Datengruppen in die Nachrichten eingebunden: Anforderungsvariablen und Geschäftsprozessvariablen. Anforderungsvariablen enthalten Informationselemente, die während des Registrierungsprozesses (normalerweise beim Ausfüllen eines Formulars durch den Benutzer) erfasst werden. Geschäftsprozessvariablen hingegen enthalten Informationen, die programmseitig durch Geschäftsprozesse und durch den Regel-Exit definiert werden. Diese Variablen werden als Gruppen URL-codierter Name-/Wert-Paare folgendermaßen zu Nachrichten hinzugefügt:

- request_vars= —URL-encoded set of name=value pairs from enrollment form
- bp_vars= —URL-encoded set of name=value pairs set by business processes

Sowohl die für eine verarbeitete Anforderung definierten Anforderungsvariablen als auch die entsprechenden Geschäftsprozessvariablen werden in Anforderungssätzen in der Registrierungsdatenbank verwaltet. Nach dem Hinzufügen zu einem Anforderungssatz in der Datenbank werden Anforderungsvariablen niemals mehr durch Geschäftsprozesse geändert. Geschäftsprozessvariablen können hingegen durch Geschäftsprozesse, durch Administratoren (Registratoren), die RA Desktop verwenden, sowie durch den Regel-Exit selbst geändert werden.

Registrierung

Als Registrierung bezeichnet man den Prozess der Erteilung eines digitalen Zertifikats an eine Person oder Entität. Unter Tivoli PKI wertet vor der Registrierung entweder ein Programm oder der Registrator die Informationen der Registrierungsanforderung aus. Anschließend erstellt die Registrierungsstelle (RA) von Tivoli PKI unabhängig davon, ob die Anforderung genehmigt oder zurückgewiesen wurde, einen Datensatz für die Anforderung in der Registrierungsdatenbank. Wenn die Anforderung genehmigt wird, stellt der Zertifikatsaussteller (CA) von Tivoli PKI das gewünschte Zertifikat aus.

Unternehmensregel

Wenn ein Programm oder ein Registrator eine Registrierungsanforderung auswertet, werden die geltenden Unternehmensregeln auf bestimmte Daten innerhalb der Registrierungsinformationen angewendet. Die Informationen, die von einem Programm ausgewertet werden können, sind weniger komplex als die Informationen, die ein Administrator auswertet. Die Werte, z. B. die Angabe der Mindestanzahl von Jahren, die ein Antragsteller ohne Wohnortwechsel sein muss, sind im Allgemeinen präzise. Tivoli PKI ermöglicht Ihrem Unternehmen, einem solchen Programm Regelinformationen zur Verfügung zu stellen. Das Programm verwendet diese Informationen zur Durchführung der Auswertungen.

Ein Programm, das einen Registrator bei seiner Tätigkeit unterstützt, wird als Regel-Exit bezeichnet. Tivoli PKI stellt einen Beispiel-Regel-Exit zur Verfügung, der zur automatischen Genehmigung von Anforderungen dient.

Dieser Regel-Exit kann in der vorinstallierten Version verwendet werden. Er besteht aus einer Gruppe von Geschäftsprozessobjekten (BPOs = Business Process Objects), die in einer angegebenen Reihenfolge ausgeführt werden. Jedes BPO implementiert eine bestimmte Operation. Es dient zum Editieren von Elementen der Registrierungsanforderungen und automatisiert die Genehmigung.

Bei Bedarf können Sie den Regel-Exit anpassen. Hierdurch können Sie Ihre Unternehmensregeln bei der Anforderungsverarbeitung anwenden und folgende Operationen ausführen:

- Anpassen des Exits und Hinzufügen eigener Verarbeitungsprozeduren.
- Erstellen neuer Regel-Exits auf der Basis des bereitgestellten Beispiels. Ihr Unternehmen kann diese Exits während der Registrierung zum Aufrufen eigener Programme einsetzen.

Das IBM Redbook *Working with Business Process Objects for Tivoli SecureWay PKI*, SG24-6043-00 enthält Anleitungen zum Entwickeln und Anpassen von Geschäftsprozessobjekten (BPOs) im Einklang mit Ihren individuellen Geschäftsanforderungen.

Datensatzattribute

Die Attribute eines Datensatzes in der Registrierungsdatenbank sind Variablen, die zur Beschreibung der Registrierungsanforderung dienen. Bei positiv beantworteten Anforderungen enthalten die Variablen auch eine Beschreibung des erteilten Zertifikats. Andere Attribute definieren Verarbeitungsvariablen, die Ihr Unternehmen dabei unterstützen, seine Unternehmensregeln durchzusetzen. Bestimmte Attribute und ihre zugehörigen Werte können vom Registrator über RA Desktop angezeigt werden.

Registrierungsstellen

Unter Tivoli PKI ist die Registrierungsstelle (RA = Registration Authority) als Serveranwendung implementiert. Sie dient zur Ausführung der folgenden Verwaltungsaufgaben, die bei der Benutzerregistrierung ausgeführt werden müssen:

- Bestätigen der Benutzeridentität
- Prüfen der Berechtigung eines Antragstellers für ein Zertifikat mit den gewünschten Attributen und Berechtigungen
- Genehmigen oder Zurückweisen von Anforderungen zum Erstellen oder Widerrufen von Zertifikaten
- Prüfen des Antragstellers auf das Vorhandensein des zugehörigen privaten Schlüssels für den öffentlichen Schlüssel im Zertifikat

Unter Tivoli PKI stellt die Registrierungsstelle den Rahmen zur Unterstützung eines breiten Spektrums an Registrierungsaktionen bereit. Sie können die Registrierungsfunktion auf die Regeln und Richtlinien Ihres Unternehmens abstimmen.

Registrierungsdatenbanken

In der Registrierungsdatenbank von Tivoli PKI werden Registrierungssätze gespeichert. Bei der Registrierungsdatenbank handelt es sich um eine relationale Datenbank, die unter IBM DB2 Universal Database erstellt wird. Tivoli PKI kann die gespeicherten Datensätze verschlüsseln. Allerdings kann ein berechtigter Registrator über RA Desktop die meisten Registrierungsinformationen lesen.

Registrierungsdomänen

Jedes Tivoli PKI-System unterstützt als Server eine einzige Registrierungsdomäne. Diese Domäne definiert die Unternehmensregeln, Zertifikatsregeln und Ressourcen, die bei der Registrierung und Zertifizierung in Ihrem Unternehmen benötigt werden. Benutzer, die auf eine Ressource zugreifen wollen, müssen in der Domäne für die gewünschte Ressource registriert sein.

Nach der Installation der RA-Software kann Ihr Unternehmen seine Tivoli PKI-Registrierungsfunktion konfigurieren. Es kann die Verwendung beliebiger Sprachen und Regeln, die von der Registrierungsstelle unterstützt werden, angeben. Die Webadresse für den Zugriff auf die Registrierungsfunktion besteht aus dem Domänennamen, der Sprache und dem Installationspfad.

Lautet beispielsweise der Name Ihres öffentlichen Webservers 'MyPublicWebServer' und der Domänenname 'MyDomain', können Sie über die folgende Webadresse auf die Registrierungsfunktion zugreifen:

`http://MyPublicWebServer/MyDomain/`

Ein Tivoli PKI-System umfasst eine standardmäßige Java Server-Seite (index.jsp) für Ihre Registrierungsfunktion. Diese Seite wird unter der Webadresse für die Registrierungsdomäne angezeigt und stellt Services für die Registrierung zur Verfügung. Zukünftige Benutzer können diese Webseite aufrufen, um ein Zertifikat anzufordern, Anforderungen für eine Vorabregistrierung zu stellen und eigene Browserzertifikate zu erneuern oder zu widerrufen.

Sie können verschiedene Funktionen und Merkmale Ihrer Registrierungsdomäne anpassen. Hierzu gehören z. B. ihr Name sowie die Art und Weise, in der die Registrierungsfunktion die verschiedenen Aufgaben der Registrierung und Zertifizierung verarbeitet.

Registrierungssätze

Jede Zertifikatsanforderung wird in Form eines Registrierungsformulars gestellt, das an die Registrierungsstelle von Tivoli PKI übergeben wird. Jede Registrierungsanforderung wird in einem Datensatz in der Registrierungsdatenbank festgehalten. Aktualisierungen an diesem Datensatz spiegeln alle Aktionen zu der Anforderung und auch deren Zurückweisung wider. Wenn ein Zertifikat erstellt wird, protokolliert dieser Datensatz außerdem alle Ereignisse, die mit dem Zertifikat in Zusammenhang stehen. Der Registrierungssatz enthält also alle Ereignisse, die während der Gültigkeitsdauer einer Anforderung sowie des zugehörigen Zertifikats eingetreten sind.

Zertifizierung

Als Zertifizierung bezeichnet man die Erstellung eines digitalen Zertifikats für eine Entität oder Person. Unter Tivoli PKI wird die Zertifizierung nur nach der Auswertung und Genehmigung einer Registrierungsanforderung durchgeführt. Als Ergebnis der Registrierung und Genehmigung stellt der CA anschließend die gewünschten Zertifikate aus. Bei Tivoli PKI stimmt der ausgestellte Zertifikatstyp mit den Unternehmensregeln Ihres Unternehmens überein.

Tivoli PKI unterstützt die gegenseitige Zertifizierung, bei der CAs, die sich als gesichert betrachten, ihre Zertifikate gegenseitig als Nachweis der Authentizität akzeptieren. Tivoli PKI unterstützt außerdem eine CA-Hierarchie. CAs betrachten diejenigen CAs als gesichert, die innerhalb der Hierarchie über ihnen stehen und akzeptieren die Zertifikate dieser CAs als Nachweis der Authentizität.

Zertifikatsaussteller

Unter Tivoli PKI ist der Zertifikatsaussteller (CA = Certificate Authority) als Server-Programm implementiert, das zur Tivoli PKI-Registrierungsfunktion gehört. Es dient zum Ausstellen digitaler Zertifikate in Übereinstimmung mit den Regeln Ihres Unternehmens.

Der CA verfügt über Schnittstellen zur RA und verwaltet den Zertifizierungsvorgang. Er fungiert als vertrauenswürdiger Dritter und stellt sicher, dass Benutzer, die im e-business tätig sind, sich gegenseitig vertrauen können. Er bürgt mittels der von ihm ausgestellten Zertifikate für die Identität von Benutzern. Das Zertifikat enthält einen öffentlichen Schlüssel, mit dem andere Benutzer verschlüsselte Daten an den Benutzer senden können, dem das Zertifikat gehört. Der private Schlüssel, der zu dem im Zertifikat definierten öffentlichen Schlüssel gehört, ermöglicht dem Benutzer die Unterzeichnung von Daten.

In einem solchen Sicherheitsmodell hängt die Vertrauenswürdigkeit der Kommunikationsteilnehmer von dem Vertrauen ab, das in den Zertifikatsaussteller gesetzt werden kann, der die Zertifikate ausstellt. Um die Integrität eines Zertifikats sicherzustellen, leistet der CA im Rahmen der Erstellung eine digitale Unterschrift auf dem Zertifikat. Durch Versuche, das Zertifikat zu manipulieren, wird die Unterschrift ungültig und das Zertifikat unbrauchbar.

Weitere Informationen zum Zertifikatsaussteller (CA) von Tivoli PKI finden Sie im Handbuch *Tivoli PKI Systemverwaltung*.

Zertifikatswiderrufslisten (CRL)

Die Tivoli PKI-Registrierungsstelle kann so konfiguriert werden, dass entweder einzelne Zertifikatswiderrufslisten (CRLs = Certificate Revocation Lists) oder CRL-Verteilungspunkte in regelmäßigen Zeitabständen publiziert werden. Bei beiden Konfigurationen werden Zertifikate aufgelistet, die nicht mehr gültig sind, sodass deren Eigner bei Vorlage nicht mehr authentifiziert werden können. Wird Tivoli PKI so konfiguriert, dass das System CRL-Verteilungspunkte ausgibt, müssen von der Auswertungsanwendung weniger Informationen abgerufen werden, um den Zertifikatseigner zu authentifizieren.

Alle Zertifikatsaussteller, Registrierungsstellen und Anwendungen können auf die CRL-Informationen zugreifen, um festzustellen, ob ein Zertifikat widerrufen wurde. Durch das Veröffentlichen der CRL-Informationen bietet die Registrierungsstelle von Tivoli PKI Schutz gegen den unerlaubten Systemzugriff nicht berechtigter Benutzer auf die gesicherten Anwendungen Ihres Unternehmens.

Verzeichnisse (Directory)

Das Verzeichnis, das von Tivoli PKI zum Speichern von Zertifikaten verwendet wird, ist das IBM Directory. Dieses Verzeichnis kann von Ihrem Unternehmen speziell für Tivoli PKI definiert werden. Alternativ hierzu kann auch ein zuvor installiertes und bereits von anderen Anwendungen benutztes Verzeichnis festgelegt werden.

Als Protokoll, das für den Zugriff auf dieses Verzeichnis eingesetzt wird, verwendet Tivoli PKI LDAP (Lightweight Direct Access Protocol).

Registrierte Namen

Der registrierte Name (DN = Distinguished Name) ist ein Element des Directory-Eintrags für ein digitales Zertifikat. Er dient zur eindeutigen Identifizierung der Position dieses Eintrags innerhalb der hierarchischen Directory-Struktur.

Zertifikate

Bei einem Zertifikat handelt es sich um einen digitalen Identitätsnachweis, der von einem CA unterzeichnet wird, der für die Identität des Zertifikatseigners bürgt. Der Eigner des Zertifikats kann sich mit diesem authentifizieren, Daten unterzeichnen und verschlüsseln sowie an der gesicherten Kommunikation mit Hilfe von Protokollen wie z. B. SSL (Secure Socket Layer) teilnehmen. Unter Tivoli PKI können Entitäten, d. h. Benutzer, Server und andere Einheiten (z. B. Router), Zertifikate anfordern.

Tivoli PKI unterstützt X.509v3-Zertifikate der folgenden Kategorien:

- Browser-Zertifikate
- Server-Zertifikate
- Einheitenzertifikate
- Zertifikate für den Zugriff auf PKIX-kompatible Anwendungen
- Gegenseitig ausgestellte Zertifikate für CAs

Eine Tivoli PKI-Standardinstallation stellt eine Vielzahl von Zertifikatstypen zum Einsatz in Anwendungen wie z. B. SSL, S/MIME und IPSec bereit. Antragsteller können Zertifikate anfordern, die ihren individuellen Anforderungen entsprechen. Unter „Zertifikatstypen“ auf Seite 62 werden die verschiedenen Zertifikatstypen beschrieben.

Bei der Anforderung eines Zertifikats starten Sie einen Gültigkeitszeitraum, der den gesamten Verarbeitungszeitraum dieses Identitätsnachweises umfasst. Dieser Gültigkeitszeitraum endet, wenn das Zertifikat widerrufen oder sein Ablaufdatum erreicht wird.

Wenn ein Zertifikat erneuert wird, erstellt das System ein neues Zertifikat, das mit dem registrierten Namen (DN) des Originaldokumentes übereinstimmt.

Browserzertifikate

Bei einem Browser-Zertifikat handelt es sich um einen digitalen Identitätsnachweis, der normalerweise von einem Web-Browser in einer verschlüsselten Datei gespeichert wird. Tivoli PKI unterstützt die Browser Netscape und Microsoft Internet Explorer. Bestimmte Anwendungen ermöglichen es dem Zertifikatseigner, die erforderlichen Schlüssel auf einer Smart-Card oder einem anderen Datenträger zu speichern. In einem Tivoli PKI-System können Benutzer ein Browser-Zertifikat direkt über ihren Web-Browser anfordern. Zu einem späteren Zeitpunkt können Sie dann bei Bedarf auf die Registrierungs-Web-Seite zurückkehren, um das Zertifikat zu erneuern oder zu widerrufen.

CA-Zertifikate

Alle Browser, Server und Einheiten, die über ein Zertifikat zur Vorlage bei der Registrierungsstelle von Tivoli PKI verfügen, müssen auch ein kompatibles CA-Zertifikat besitzen. Dieses Zertifikat wird für die Authentifizierung der Kommunikation mit Servern benötigt, die über Zertifikate verfügen, die vom CA von Tivoli PKI ausgestellt wurden.

In Ihrem Browser muss ein Tivoli PKI-CA-Zertifikat vorliegen, damit Sie mit den gesicherten Tivoli PKI-Registrierungsservices arbeiten können. Sie können dieses Zertifikat abrufen, wenn Sie zum ersten Mal die Registrierungswebseiten von Tivoli PKI aufrufen. Anschließend können Sie immer, wenn Sie ein Zertifikat von den Registrierungsservices anfordern, auch das entsprechende kompatible CA-Zertifikat herunterladen.

Wenn Sie z. B. ein SSL-Browserzertifikat mit einem Gültigkeitszeitraum von zwei Jahren anfordern, können Sie ein CA-Zertifikat empfangen, das mit diesem kompatibel ist.

Anmerkung: Frühere Releases von Netscape konnten Site-Zertifikate akzeptieren, die von einem Tivoli PKI-Server vorgelegt wurden. Diese Zertifikate wurden sowohl für die server-authentifizierte als auch die client-authentifizierte Kommunikation mit diesem Server akzeptiert. Beim neuesten Release von Netscape ist jedoch für client-authentifizierte Sitzungen ein CA-Zertifikat erforderlich.

Server- oder Einheitenzertifikate

Wenn dies zu ihrem Aufgabenbereich gehört, können bestimmte Personen Zertifikate für einen Server (z. B. einen Web-Server) oder eine andere Einheit anfordern. Hierzu wird das Browser-Registrierungsformular von Tivoli PKI verwendet.

Die Server bzw. Einheiten, für die das Zertifikat benötigt wird, müssen das Anforderungsformat PKCS #10 verwenden.

Zertifikatserweiterungen

Zertifikatserweiterungen sind optionale Elemente im Format eines X.509v3-Zertifikats. Diese Erweiterungen ermöglichen die Einbindung zusätzlicher Felder in das Zertifikat. Tivoli PKI stellt eine Gruppe von Zertifikatserweiterungen bereit, um Ihrem Unternehmen das Anpassen der selbst ausgestellten Zertifikate zu ermöglichen.

Registatoren, die einen Registrierungssatz in RA Desktop anzeigen, können diese Felder sehen, wenn sie die Verarbeitungsattribute aufrufen. In bestimmten Fällen kann der Registrator die zugehörigen Werte auch aktualisieren.

Erneuerbarkeit

Die Erneuerbarkeit eines Zertifikats ist eines der Merkmale, die über RA Desktop geändert werden können:

- Wenn ein Zertifikat erneuerbar ist, kann der Eigner einen Antrag für ein neues Zertifikat einreichen, solange das alte Zertifikat noch gültig ist. Die Verfügbarkeit eines erneuerbaren Zertifikats vereinfacht den Registrierungsprozess und den hierbei erforderlichen Aufwand.
- Kann ein Zertifikat nicht erneuert werden, muss der Eigner warten, bis dessen Gültigkeit abgelaufen ist und anschließend eine erneute Registrierung beantragen, wenn das Zertifikat weiterhin benötigt wird. Bei der Registrierung müssen wie beim ersten Mal alle Informationen nochmals bereitgestellt werden.

Benutzer mit erneuerbaren Browserzertifikaten können die Erneuerung auf der Registrierungswebseite anfordern.

Zertifikatsprofile

Tivoli PKI stellt leistungsstarke und flexible Funktionen zum Anpassen des spezifischen Inhalts der verschiedenen Zertifikate bereit, die mit Hilfe von Zertifikatsprofilen ausgestellt werden. Ein Zertifikatsprofil definiert die Regeln für die Zusammenstellung von Zertifikaten, die zur Unterzeichnung an den CA-Server weitergeleitet werden. Diese Regeln sind textbasiert und können mit einem konventionellen Texteditor verwaltet werden. (Informationen zum Editieren von Textdateien, die Nicht-ASCII-Zeichen im Unicode- oder UTF-8-Format enthalten, finden Sie in „Anpassungs-Tools“ auf Seite 41.)

Diese Regeln decken die meisten Elemente eines Zertifikats ab, die mit der Registrierungs-funktion definiert werden können. Hierzu gehören auch die folgenden Attribute:

- Name des Zertifikatsgegenstands
- Gültigkeitsbeginn
- Gültigkeitsende
- Zertifikatserweiterungen
- Schlüsselnutzung
- Erweiterte Schlüsselnutzung
- Alternativname für den Zertifikatsgegenstand
- Zertifikatsregeln
- Private Erweiterungen
- Zu verwendendes Directory-Schema

Eine einzelne Datei enthält alle Profildefinitionen, die innerhalb einer Registrierungsdomäne verwendet werden. Die Standarddatei trägt den Namen 'certificate_profiles.cfg' und ist im Unterverzeichnis 'etc' für Ihre Registrierungsdomäne gespeichert.

- Unter AIX lautet der Standardinstallationspfad
/usr/lpp/iau/pkrf/Domains/*YourDomain*/etc.
- Unter Windows NT lautet der Standardpfad c:\Program Files\IBM\Trust
Authority\pkrf\Domains*YourDomain*\etc.

Diese Datei ist in unterschiedliche Abschnitte für die verschiedenen Profile aufgeteilt. Definitionen am Anfang der Datei gelten global, es sei denn, sie werden von den Definitionen in einem bestimmten Profil überschrieben. Globale Regeln bieten Ihnen eine Möglichkeit, den Dateiinhalt kleiner zu halten, als wenn die Regeln in allen Profilen wiederholt werden müssen.

Profilverarbeitung

Wenn eine Zertifikatsanforderung ausgefüllt und genehmigt ist, wird sie zur Verarbeitung an den RA-Server weitergeleitet. Der RA-Server ruft die Anforderung aus der RA-Datenbank ab und erstellt aus dem Inhalt der RA-Datenbankanforderung (Anforderungs- und Geschäftsprozessvariablen) einen Pool mit Datenvariablen. Alle Geschäftsprozessvariablen überschreiben die entsprechenden Anforderungsvariablen. Dieser Ansatz ermöglicht es, dass die Regel-Exits Ihres Unternehmens auf den Inhalt von Zertifikaten angewendet werden. Hierzu werden entsprechende Definitionen in die Geschäftsprozessvariablen eingebunden.

Der RA-Server prüft die Anforderung auf das Vorhandensein einer PKIX-Zertifikatsanforderung (PKCS #10) oder eines Netscape-SPK-Objekts (SPK = Signed Public Key). Wird eine dieser Komponenten festgestellt, werden sie über eine syntaktische Analyse in eine andere Variablengruppe eingelesen. Momentan werden vom RA-Server nur die folgenden Werte extrahiert:

- Name des Zertifikatsgegenstandes
- RDNs für den Namen des Zertifikatsgegenstandes
- Zertifikatserweiterungen
- Informationen zu den öffentlichen Schlüsseln

Beachten Sie hierbei, dass Anforderungen des Browsers Netscape nur den öffentlichen Schlüssel und eine Abfrage in ihren Anforderungsobjekten bereitstellen. Darüber hinaus können PKCS #10- und PKIX-Anforderungsobjekte optional eine Gruppe von Definitionen für Zertifikatserweiterungen enthalten.

Das Zertifikatsprofil selbst definiert zusätzliche Werte in Form von Regeln und Konstanten. Diese Regeln und Konstanten stellen eine weitere Gruppe von Variablen bereit, die bei der Zusammenstellung des Zertifikats eingesetzt werden. Bei der Profilverarbeitung werden immer die Definitionen im Zertifikatsprofil gegenüber den Definitionen in anderen Datenquellen bevorzugt behandelt.

Zu diesem Zeitpunkt beginnt der RA-Server mit der Zusammenstellung des Zertifikats. Er ruft aus dem Profil die Regeln für die Attribute 'subjectName', 'validityNotBefore' und 'validityNotAfter' sowie für die Erweiterungen ab. Diese Regeln definieren eine Reihe von symbolischen Ersetzungen, die verwendet werden sollen. Die Ersetzungsregeln geben an, welcher Datenpool nach einem bestimmten Wert durchsucht werden soll. Kann der gesuchte Wert in einem Datenpool nicht gefunden werden, definiert die Regel einen zu verwendenden Standardwert. Dieser Standardwert kann wiederum einen anderen Datenpool angeben. Dieses Muster kann solange wiederholt werden, bis alle Datenpools geprüft wurden. In diesem Fall kann dann eine Literalkonstante definiert oder ein Leerwert angenommen werden.

Nachdem die Zertifikatsanforderung an den CA-Server gesendet und das Zertifikat ausgestellt wurde, empfängt der RA-Server das Zertifikat und speichert es in einer Datenbank, damit das Zertifikat auf Anforderung des Benutzers geliefert werden kann. Wenn der Benutzer das Zertifikat abrufen, prüft Approver Framework die Anforderung, um alle erforderlichen Einträge im Verzeichnis (Directory) zu erstellen. Die zum Erstellen der Einträge verwendeten Datentypen werden durch die in einem bestimmten Zertifikatsprofil enthaltenen Regeln und Definitionen gesteuert.

Momentan werden von Approver Framework nur die folgenden Werte extrahiert:

- Directory-Objektklassen
- Directory-Attribute

Im Allgemeinen führen Leerwerte dazu, dass der RA-Server oder Approver Framework die Definition ignoriert oder aus dem Zertifikatsobjekt, das zusammengestellt wird, löscht. Wenn die Regel für das Attribut 'subjectName' eines Zertifikats z. B. eine Definition für 'locality' enthält, in den Datenpools oder im Profil jedoch kein Wert für 'locality' gefunden wurde, wird der RDN aus dem generierten Attribut 'subjectName' des Zertifikats gelöscht.

Die bevorzugte Verarbeitungsreihenfolge bei der Symbolersetzung wird im Profil definiert. Sie können diese entsprechend Ihren individuellen Anforderungen anpassen. Die Standardpriorität bevorzugt Daten aus der Registrierungsanforderung gegenüber Werten, die in PKIX- und PKCS #10-Objekten gespeichert sind. Diese Prioritätenregelung stellt sicher, dass im Zertifikat immer die ursprünglichen Registrierungsinformationen verwendet werden, unabhängig davon, ob vom Endbenutzer noch kurzfristige Änderungen an den PKIX- oder PKCS #10-Anforderungsobjekten vorgenommen wurden. Ein Antragsteller kann z. B. in der PKIX-Anforderung einen anderen als den bei der Vorabregistrierung genehmigten Namen verwenden.

Im Folgenden ist ein Beispiel einer Gruppe von Regeln aufgeführt, die die Definition des Feldes 'subjectName' (für den Namen des Zertifikatsgegenstands) eines möglichen Zertifikats steuern:

```
CN_default=%request.first_name% %request.last_name%
CN_pkcs10=%pkcs10.CN,default(%%CN_default%%)%
CN=%request.CN,default(%%CN_pkcs10%%)%
SubjectName=/C=US/O=Your Company/OU=Your Department/CN=%%CN%%
```

In diesem Beispiel besteht das Attribut 'subjectName' des Zertifikats aus vier RDNs. Die RDNs für das Land (C = Country), die Firma (O = Organization) sowie die Abteilung (OU = Organizational Unit) sind fest codiert. Das Feld für den allgemeinen Namen (CN = Common Name) wird aus den Daten abgeleitet, die in der Anforderung enthalten sind. Die Verarbeitungsregeln weisen den RA-Server mit der Zeichenfolge 'request.CN' an, in den Daten der Registrierungsanforderung zuerst nach einer CN-Definition zu suchen. Wird dort keine Definition gefunden, sucht der RA-Server (entsprechend dem Wert 'pkcs10.CN') in der PKCS- oder PKIX-Nachricht nach der benötigten Definition. Wird nirgends eine CN-Definition gefunden, erstellt der RA-Server den allgemeinen Namen anhand des Vor- und Nachnamens des Antragstellers.

Anmerkung: Es ist wichtig zu verstehen, dass der RA-Server in jedem Fall versucht, die Zertifikatsanforderung komplett auszufüllen. Dies ist auch dann der Fall, wenn ein fehlerhaftes Profil oder fehlerhafte Eingabedaten festgestellt werden. Werden fehlende oder fehlerhafte Daten identifiziert, verwendet das System die im Profil definierten Standardwerte. Dies kann unter Umständen dazu führen, dass das Zertifikat nicht die erwarteten Werte enthält. In extremen Fällen kann es auch passieren, dass die Zertifikatsanforderung vom CA-Server zurückgewiesen wird. Sie sollten sicherstellen, dass Ihre Profildefinitionen immer gültige Zertifikate und Ergebnisse für die verwendete Umgebung und die angewendeten Regeln generieren.

Organisation, Inhalt und Struktur von Profilen

Bei der Zertifikatsprofildatei handelt es sich um eine Textdatei mit zwei oder mehr Abschnitten. Alle Definitionen und Regeln, die vor dem Abschnitt eines spezifischen Zertifikatsprofils angegeben sind, gelten global. Das bedeutet, dass die im globalen Abschnitt gefundenen Definitionen für alle Profile angewendet werden, es sei denn, sie werden von profilspezifischen Definitionen überschrieben. Der globale Abschnitt ermöglicht das zentrale, profilübergreifende Konsolidieren von Definitionen. Hierdurch wird das Erstellen von Profilen vereinfacht und die Dateigröße reduziert, da unnötige Redundanzen eliminiert werden. Im Allgemeinen werden Felder wie 'subjectName' global definiert.

Im Folgenden sind verschiedene Beispiele für globale Definitionen aufgeführt:

```
; --- Define default PKIX EE/CA Preregistration values
;
; 72 hours
prereg_expiresInSeconds=259200
prereg_client=EE
prereg_annotation=RA Server

; --- Define enrollment request expiration period, this is
; --- the period after creation of the request record in DB
request_expires_in_hours=72

; --- Define validityNotBefore values
validityNotBefore_range=0,30
validityNotBefore_default=0
```

Nach dem globalen Abschnitt werden ein oder mehrere Zertifikatsprofile definiert. Ein Zertifikatsprofil wird durch seinen in eckigen Klammern ([]) geschriebenen Namen gekennzeichnet. Im folgenden Beispiel wird ein Zertifikatsprofil für ein S/MIME-Zertifikat mit einer Gültigkeitsdauer von einem Jahr definiert:

```
[S/MIMECert1Year]
```

Leerzeilen und Zeilen, die mit einem Semikolon (;) beginnen, werden ignoriert. Hierbei werden die mit einem Semikolon beginnenden Zeilen als Kommentare interpretiert. Beispiel:

```
; --- S / M I M E C e r t 1 Y e a r ---
```

Im Folgenden ist ein Beispiel für eine vollständige Profildefinition aufgeführt:

```
; --- S / M I M E C e r t 1 Y e a r ---
[S/MIMECert1Year] display_name=S/MIME Certificate - Valid for 1 Year
required_fields=first_name,last_name,email_address

; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,subjectAltName,
certificatePolicies
keyUsage=digitalSignature&keyEncipherment
extendedKeyUsage=emailProtection
subjectAltName=rfc822Name=%%MAIL%%
; subjectName
subjectName=/C=%%C%%/O=%%O%%/OU=%%OU%%/ST=%%ST%%/L=%%L%%/PC=%%PC%%
/T=%%T%%/CN=%%CN%%+MAIL=%%MAIL%%

; --- Define validityNotAfter values
validityNotAfter_range=0,365
validityNotAfter_default=365
```

Anmerkung: Beachten Sie hierbei, dass durch die Formatierung des vorliegenden Dokuments die Definitionen für 'extensions_required' und 'subjectName' möglicherweise mehr als eine Zeile umfassen. Im tatsächlichen Zertifikatsprofil ist dies jedoch nicht zulässig. Alle Regeldefinitionen müssen sich in jeweils einer Zeile befinden.

Die Regel 'display_name' definiert den Profiltitel, der dem Endbenutzer während der Registrierung und in RA Desktop angezeigt wird. Die Regel 'required_fields' definiert die Felder, die der Endbenutzer im Registrierungsgerüst dieses Profils angeben muss.

Bei Ländern, in denen zur Darstellung des Attributs 'display_name' Nicht-ASCII-Zeichen erforderlich sind (z. B. für Japanisch, Chinesisch, Deutsch, Französisch etc.), wird der Wert im UTF-8-codierten Unicode-Format angegeben. Unicode/UTF-8 erlaubt das universelle Codieren von Zeichen und ermöglicht Tivoli PKI die gleichzeitige Unterstützung mehrerer Sprachen auf dem selben System und sogar innerhalb eines Zertifikatsprofils. Wenn die Profildatei UTF-8-codierte Daten enthält, muss beim Editieren mit besonderer Vorsicht vorgegangen werden, um die Beschädigung der UTF-8-Werte zu verhindern. (Informationen zu den empfohlenen Editoren finden Sie in „Anpassungs-Tools“ auf Seite 41.) In den meisten Fällen sollten Sie zuerst die Datei in eine native Codepage konvertieren, diese dann editieren und sie anschließend zurück ins UTF-8-Format konvertieren.

Ein weiterer wichtiger Punkt, der unbedingt berücksichtigt werden muss, ist die Schreibung der in der Profildatei enthaltenen Felder. Bei der Verwendung der Profilwerte durch den RA-Server muss die Groß-/Kleinschreibung beachtet werden. Die exakte Schreibung ist hierbei sehr wichtig. Falsch geschriebene Feldnamen führen im Allgemeinen zu fehlenden Definitionen. Abhängig vom verwendeten Profil können die fehlenden Definitionen dazu führen, dass ein erforderlicher Wert nicht definiert werden kann und dass deswegen möglicherweise die gesamte Zertifikatsanforderung zurückgewiesen wird.

Substitutionsvariablen in Profilen

Die Definition von Profilregeln kann ein Symbol oder mehrere Symbole enthalten, dessen bzw. deren Wert aus dem Variablenpool abgerufen werden kann, der vom RA-Server oder von Approver Framework während der Profilverarbeitung erstellt wird. Substitutionssymbole werden durch zwei aufeinander folgende Prozentzeichen (%%) vor und nach dem Namen gekennzeichnet. Beispiel:

```
SubjectName=/CN=%%request.CN%%
```

In diesem Beispiel definiert 'request.CN' eine Substitutionsvariable. Die Variable CN wird aus den Registrierungsdaten abgerufen, die in der RA-Datenbank gespeichert sind.

Wird die Variable 'request.CN' in diesem Variablenpool nicht definiert, kann dem Attribut 'subjectName' kein Wert zugeordnet werden. Um dieses Problem zu lösen, werden bei der Profilverarbeitung Standardwerte für alle Substitutionssymbole bereitgestellt. Beispiel:

```
CN_default=%%request.first_name%% %%request.last_name%%
CN_pkcs10=%%pkcs10.CN,default(%%CN_default%%)%%
SubjectName=/CN=%%request.CN%%,default(%%CN_pkcs10%%)%%
```

Diese Definitionen weisen den RA-Server an, die CN-Definition zuerst in den Registrierungsdaten zu suchen. Wird die Definition dort nicht gefunden, durchsucht er als Nächstes die PKCS #10-Komponente nach einer CN-Definition. Schlägt die Suche auch dort fehl, erstellt der RA-Server eine entsprechende Definition und verwendet hierzu den aus den Registrierungsdaten abgerufenen Vor- und Nachnamen des Antragstellers.

Kann ein Variablenwert durch die im Profil definierten Regeln nicht aufgelöst werden, verarbeitet der RA-Server das zugehörige Feld so, als ob es eine Leerzeichenfolge enthalten würde. Abhängig von der Verwendung der Variablen kann diese Vorgehensweise unter Umständen zu Problemen führen. Wenn im vorherigen Beispiel dem Attribut 'CN_default' kein Wert zugeordnet wird, verfügt das Attribut 'subjectName' des Zertifikats über keinen allgemeinen Namen (CN). Hierdurch wird die Zertifikatsanforderung vom Zertifikatsaussteller (CA) voraussichtlich zurückgewiesen (wenn 'subjectAltName' keinen Namen definiert).

Der RA-Server und das Approver Framework erstellen die folgenden Variablengruppen zur Verwendung als Substitutionsvariablen:

- **Profildefinitionen** - die Paare aus Name und Wert, die in der Zertifikatsprofildatei enthalten sind.
- **Anforderungswerte** - die Paare aus Name und Wert der Registrierungsdaten, die in der RA-Datenbank enthalten sind.
- **pkcs10-Werte** - die Paare aus Name und Wert für Informationen von einem PKCS #10- oder PKIX-Objekt, das der Zertifikatsanforderung zugeordnet ist.
- **subjectName-Werte** — die Paare aus Name und Wert, die im Namen des Zertifikatsgegenstands ('subjectName'; erst nach Ausgabe des Zertifikats verfügbar) enthalten sind. **(Nur Approver Framework)**

Die **Profildefinitionen** haben gegenüber allen anderen, in der Anforderung oder den pkcs10-Variablenpools definierten Werten Priorität. Profildefinitionen stammen immer aus dem globalen Abschnitt des Zertifikatsprofils und den für das Zertifikatsprofil spezifischen Abschnitten der Profildatei.

Die **Anforderungswerte** stammen aus den Registrierungs- und Geschäftsprozessvariablen, die im RA-Datenbankobjekt gespeichert sind, das der verarbeiteten Zertifikatsanforderung zugeordnet ist. Beim Erstellen des Anforderungsvariablenpools mischt der RA-Server die Registrierungs- und Geschäftsprozessvariablen so, dass alle in der Gruppe der Geschäftsprozessvariablen definierten Felder die entsprechenden Einträge in den Registrierungsvariablen überschreiben. Dieser Ansatz ermöglicht Ihnen Regel-Exits die Steuerung der Daten, die für die Profilverarbeitung verwendet werden.

Die **pkcs10-Werte** stammen aus einem PKCS #10-Objekt, das möglicherweise zusammen mit der Zertifikatsanforderung übergeben wurde. Der RA-Server extrahiert das Attribut 'subjectName' und alle angeforderten Erweiterungen aus dem angegebenen PKCS #10-Objekt. Das Attribut 'subjectName' wird anschließend weiter in einzelne RDN-Felder zerlegt. Hierdurch ist es möglich, bei der Profilverarbeitung aus dem PKCS #10-Objekt nur das CN-Feld zu verwenden.

Die Werte für **subjectName** stammen aus dem Namen des Zertifikatsgegenstands des betreffenden Zertifikats. Approver Framework führt eine syntaktische Analyse des Zertifikats aus, ruft den Wert des Attributs 'subjectName' ab und zerlegt diesen Wert weiter in Schlüsselwertpaare.

Beachten Sie hierbei, dass Anforderungen des Browsers Netscape nur über ein NSPK-Objekt (NSPK = Netscape Signed Public Key) verfügen. Dieses Objekt enthält nur den öffentlichen Schlüssel des Zertifikatsgegenstands sowie eine Abfragezeichenfolge, mit der geprüft wird, ob die Entität oder Person, die den öffentlichen Schlüssel übergibt, über den zugehörigen privaten Schlüssel verfügt.

Beachten Sie hierbei, dass bei allen Feldnamen die Groß-/Kleinschreibung beachtet werden muss. Sie müssen die Namen exakt in der angegebenen Schreibweise unter Berücksichtigung der Groß-/Kleinschreibung eingeben. Die Angabe 'request.CN' stimmt z. B. nicht mit der Angabe 'request.cn' überein.

Profilregeln und -definitionen

Das Zertifikatsprofil wird mit zahlreichen Definitionen geliefert. Die im Beispielzertifikatsprofil enthaltenen Kommentare und Beispiele bieten umfangreiche Informationen zu den Regeln, die in einem Profil definiert werden können. Im vorliegenden Dokument sollen die wichtigsten Felder beschrieben werden. Zusätzliche Informationen können Sie dem zum Lieferumfang von Tivoli PKI gehörenden Beispielzertifikatsprofil entnehmen.

display_name

Dieses Feld definiert den Namen, der dem Benutzer bei der Verwendung der Tivoli PKI-Registrierungsformulare oder des RA Desktop angezeigt wird.

Beispiel:

```
display_name=S/MIME Certificate - Valid for 1 Year
```

required_fields

Dieses Attribut enthält eine durch Kommas begrenzte Liste mit Namen von Feldern, die zum erfolgreichen Ausführen des Zertifikatsprofils erforderlich sind. Die verfügbaren Felder sind unter Tivoli PKI definiert. Sie können außerdem zusätzliche Felder definieren. Es wird empfohlen, Leerzeichen zu vermeiden und zu berücksichtigen, dass bei allen Feldnamen die Groß-/Kleinschreibung beachtet werden muss.

Beispiel:

```
required_fields=first_name,last_name,email_address
```

issuerName

Dieses Attribut gibt den Namen des Zertifikatsausstellers (CA) an, an den der RA-Server die Zertifikatsanforderung zur Unterzeichnung übergibt. Dieser Wert stimmt im Allgemeinen mit dem Attribut 'subjectName' des CA-Zertifikats überein. Er muss im OSF-Format definiert werden. Es ist zwar möglich, für jedes Zertifikatsprofil einen unterschiedlichen Zertifikatsaussteller zu definieren; momentan wird von Tivoli PKI jedoch nur ein Zertifikatsaussteller pro RA-Server unterstützt. Aus diesem Grund ist es gegenwärtig am besten, 'issuerName' als globale Definition festzulegen.

Beispiel:

```
issuerName=/C=US/O=Your Company/OU=Your Organization/CN=Your CA
```

issuerDirectory

Dieses Attribut gibt die URL-Adresse an, die auf das Verzeichnis zeigt, in dem Tivoli PKI das CA-Zertifikat sowie die Zertifikate veröffentlicht, die vom Zertifikatsaussteller unterzeichnet wurden. Dieses Verzeichnis (Directory) wird zum Abrufen des CA-Zertifikats und zum Lokalisieren von Endbenutzerzertifikaten für die Verwendung durch die Registrierungs- und Genehmigungskomponente sowie den RA-Server von Tivoli PKI eingesetzt.

Beispiel:

```
issuerDirectory=ldap://your_ldap_server.yourcompany.com:389
```

subjectName

Diese Regel definiert den Inhalt eines von Tivoli PKI ausgestellten Zertifikats. Das zugehörige Feld definiert eine Reihe von RDN-Kandidaten, aus denen sich das Attribut 'subjectName' des Zertifikats zusammensetzt. Alle RDN-Felder, die nach der Symbolsubstitution keinen Wert enthalten, werden aus dem Feld entfernt, bevor der Name 'subjectName' in die Zertifikatsanforderung eingebunden wird. Hierdurch können Sie subjectName-Felder mit zahlreichen RDN-Werten definieren, die lediglich in beschränktem Umfang benutzt werden können. Beispiel:

```
C=US
O=Your Company
OU=Your Department

CN_default=%request.first_name% %request.last_name%
CN_pkcs10=%pkcs10.CN,default(%CN_default%)%
CN=%request.CN,default(%CN_pkcs10%)%

; --- subject's State or Province
ST_pkcs10=%pkcs10.ST%
ST=%request.ST%,default(%ST_pkcs10%)%

; --- Subject's Locality
L_pkcs10=%pkcs10.L%
L=%request.L%,default(%L_pkcs10%)%

; --- Subject's Postal Code
PC_pkcs10=%pkcs10.PC%
PC=%request.PC%,default(%PC_pkcs10%)%

; -- Domain Components
DOMAIN_COMPONENTS_default=
DOMAIN_COMPONENTS=%request.DomainComponents,default(%DOMAIN_COMPONENTS_default%)%

; --- Now we build the whole name
subjectName=%DOMAIN_COMPONENTS%/C=%C%/O=%O%/OU=%OU%/ST=%ST%/L=%L%/PC=%PC%/
/T=%T%/CN=%CN%
```

Wenn der Variablen 'ST' oder 'L' kein Wert zugeordnet ist, und wenn die Werte der Anforderungsvariablen 'request.first_name=John' und 'request.last_name=Doe' lauten, gilt für 'subjectName' folgendes:

```
/C=US/O=Your Company/OU=Your Department/CN=John Doe
```

x_objectclass

Diese Regel definiert die Objektklasse, die verwendet werden soll, wenn Einträge im Verzeichnis (Directory) für den RDN-Typ 'x' erstellt werden. Außerdem definiert diese Regel sowohl die erforderlichen als auch die optionalen Attribute, die beim Erstellen des Verzeichniseintrags integriert werden sollen. Die Werte dieser Attribute werden im Rahmen dieser Regel ebenfalls definiert. Die Ermittlung dieser Werte

erfolgt anhand von Symbolsubstitution. Diese Regel ermöglicht es Ihnen, den Verzeichniseintrag mit Registrierungsinformationen auszufüllen. Beispiel:

```
; --- Object Class to be used to create entries on Directory that have the
; --- following attribute.
; --- Object Class has to match a object class on the directory schema.
; --- Required Attributes refer to values required to add the entry to the directory.
; --- Optional Attributes refer to values that could be used on the creation of the entry
; --- if available on enrollment data.

; --- Example configuration if going to use diferent schema.
;CN_objectClass=inetOrgPerson,ePerson,top
;CN_objectClass_RequiredAttributes=cnAttr,snAttr
;CN_objectClass_OptionalAttributes=
; --- Describes the values on the enrollment data to be used to populate the information
; --- on the directory.
; --- The AttributeNames need to match the attribute name specified on the directory schema.
; --- The subjectName object refers to the attribute values found on the entry RDN.

cnAttr_AttributeValue=%%subjectName.CN%%
cnAttr_AttributeFormat=String
cnAttr_AttributeName=cn

snAttr_AttributeValue=%%request.last_name%%
snAttr_AttributeFormat=String
snAttr_AttributeName=sn
```

Anmerkung: Nur das Format des Attributs 'String' wird unterstützt.

validityNotBefore

Das Feld 'validityNotBefore' definiert das erste Datum, an dem das ausgestellte Zertifikat als gültig betrachtet wird. Der RA-Server unterstützt Regeln zur Angabe eines Bereiches, der angefordert werden kann, und eines Standardwertes, der bei Überschreitung dieses Bereichs verwendet wird. Darüber hinaus können die Werte in Tagen relativ zum aktuellen Datum oder als absolute Datums- und Zeitangaben angegeben werden. Beispiel:

```
; --- Define validityNotBefore values
validityNotBefore_range=0,30
validityNotBefore_default=0
validityNotBefore=%%request.validityNotBefore,default(%%validityNotBefore_default%%)%%
```

Im vorliegenden Beispiel können Endbenutzer oder die Regel-Exits des Kunden ein Zertifikat anfordern, dessen Gültigkeit sofort beginnt und für die darauf folgenden 30 Tage gilt. Wird kein Wert angegeben oder liegt der angeforderte Wert außerhalb des zulässigen Bereichs [0..30], verwendet das System den Standardwert von 0 Tagen. Null (0) Tage wird vom RA-Server als das aktuelle Datum und die aktuelle Uhrzeit in Westeuropäischer Zeit (WEZ) interpretiert.

Negative ganzzahlige Werte werden zur Definition von Datumsangaben vor dem aktuellen Datum verwendet. Der Wert -3 bedeutet z. B. 'vor 3 Tagen'. Während es möglich ist, Startdaten in der Vergangenheit anzugeben, wird dies nicht empfohlen, da der CA-Server in diesem Fall die Zertifikatsanforderung eventuell zurückweist. Sie müssen sicherstellen, dass das für 'validityNotBefore' angegebene Datum vor dem Datum liegt, das für 'validityNotAfter' definiert wird.

Beachten Sie hierbei, dass alle Datums- und Zeitangaben als Werte in Westeuropäischer Zeit (WEZ) und nicht in Lokalzeit interpretiert werden.

validityNotAfter

Das Feld 'validityNotAfter' definiert das letzte Datum, zu dem das Zertifikat noch seine Gültigkeit besitzt. Wie auch beim Feld 'validityNotBefore' kann der Wert als ganze Zahl von Tagen oder als absolutes Datum ausgedrückt werden. Beispiel:

```
; --- Define validityNotAfter values
validityNotAfter_range=0,365
validityNotAfter_default=365
validityNotAfter=%request.validityNotAfter,default(%%validityNotAfter_default%%)%%
```

In diesem Fall kann der Endbenutzer oder der Regel-Exit des Kunden anfordern, dass das Enddatum des Zertifikats in dem Bereich zwischen dem aktuellen Datum und dem darauf folgenden Jahr liegt. Wenn der angeforderte Wert über diesen Bereich hinausgeht, wird der Standardwert (ein Jahr) verwendet. Verwenden Sie keine Datums- oder Tagesangaben in der Vergangenheit (negative ganze Zahlen), da dies dazu führen kann, dass der CA die Zertifikatsanforderung zurückweist. Darüber hinaus muss der Wert für 'validityNotAfter' nach dem Wert für 'validityNotBefore' liegen.

Es gibt Situationen, in denen Sie möglicherweise unabhängig vom Ausstellungsdatum des Zertifikates ein spezifisches Enddatum definieren wollen. Dies kann z. B. bei einer Pilotimplementierung der Fall sein. Beispiel: Die Gültigkeitsdauer aller ausgestellten Zertifikate soll am Ende des Pilotprojekts am 30. November 1999 um 00:00 Uhr Westeuropäischer Zeit (WEZ) ablaufen. Im Folgenden ist eine Beispielregel aufgeführt:

```
ValidityNotAfter=1999-11-30 00:00:00
```

Wenn die Zertifikate am Ende dieses Tages ablaufen sollen, müssen Sie als Zeit 23:59:59 angeben.

Verwaltung

Zukünftige Registratoren müssen ein Zertifikat für den Web-Browser anfordern und empfangen, über den RA Desktop verwendet werden soll. Nach dem Erhalt des Browser-Zertifikats müssen sie dieses jedes Mal vorlegen, wenn sie auf RA Desktop zugreifen wollen. Um Registrierungssätze oder Anforderungen unter RA Desktop anzuzeigen oder zu bearbeiten, muss der Registrator außerdem über die entsprechenden Dateiberechtigungen verfügen.

Die Themen in diesem Abschnitt behandeln die Verwaltung von Zertifikaten.

Zugriffssteuerung

Eine Zugriffssteuerungsliste (ACL = Access Control List) dient zum Authentifizieren und Berechtigen interner Tivoli PKI-Benutzer, -Einheiten und -Softwarekomponenten. Das RA Desktop-Unterstützungs-Servlet verwendet die ACL z. B. zum Authentifizieren und Berechtigen von Registratoren für den Zugriff auf RA Desktop.

Authentifizierung und Berechtigung

Durch die Authentifizierung wird die Identität einer Person oder Entität belegt, wohingegen durch eine Berechtigung die Ausführung bestimmter Aktionen genehmigt wird. Tivoli PKI ermöglicht Ihrem Unternehmen, diese beiden Voraussetzungen zwingend anzufordern, bevor Benutzer auf gesicherte Anwendungen zugreifen können. Zertifikatseigner können im Gegenzug sicher sein, dass die benutzten Anwendungen gesichert sind.

Parallele Verwaltung

Tivoli PKI stellt eine einzelne Registrierungsdomäne zur Verfügung, in der jedoch mehrere Registratoren arbeiten können. Das Design des RA Desktop-Servlets und der Registrierungsstelle (RA) verhindert hierbei, dass ein Datensatz aktualisiert wird, während ein anderer Benutzer gerade mit diesem arbeitet. Es ist jedoch möglich, dass mehrere Registratoren gleichzeitig den selben Datensatz anzeigen.

RA Desktop

Bei RA Desktop handelt es sich um eine grafische Benutzerschnittstelle (GUI) zur Verarbeitung von Registrierungsanforderungen und Verwaltung der hierbei generierten Datensätze. Das System unterstützt den Registrator bei der Ausführung der folgenden Aufgaben:

- Auswerten von anstehenden Registrierungsanforderungen und deren Genehmigung oder Zurückweisung
- Vorbereiten von Abfragen für das Abrufen von Datensätzen zu Zertifikaten eines bestimmten Typs oder eines bestimmten Benutzers
- Prüfen der Einzeldaten eines Datensatzes
- Definieren des Gültigkeitszeitraums eines Zertifikats
- Ausführen von Aktionen zum Ändern des Status eines Zertifikats oder einer Registrierungsanforderung
- Kommentieren eines Datensatzes zur Erläuterung des Grundes für eine ausgeführte Aktion

Bei RA Desktop handelt es sich um ein sicheres Applet. Zu seiner Verwendung müssen Registratoren sich durch die Vorlage des richtigen digitalen Zertifikats authentifizieren. Ihre Berechtigung innerhalb der Registrierungsdomäne kann auf bestimmte Aufgaben beschränkt sein.

Weitere Informationen zu RA Desktop finden Sie im Handbuch *Tivoli PKI RA Desktop*.

Servlet zur Unterstützung von RA Desktop

Das RA Desktop-Unterstützungs-Servlet ist eine Tivoli PKI-Anwendung, die dazu dient, Registratoren die Services von RA Desktop zur Verfügung zu stellen. Das Servlet gibt Informationen zurück, wenn ein Registrator eine Abfrage ausführt, und aktualisiert Datensätze, wenn ein Registrator Änderungen an diesen vornimmt.

Anforderungsprofile

Tivoli PKI stellt eine Standardgruppe von Anforderungsprofilen zur Verfügung, die Ihr Unternehmen zur Vereinfachung der Registrierung und Zertifizierung verwenden kann. Ein Anforderungsprofil steuert die Attribute und die Verarbeitung einer Registrierungsanforderung. Jedes Anforderungsprofil umfasst eine Schablone für ein Zertifikat. Es gibt verschiedene Anforderungsprofile für die unterstützten Zertifikatskategorien.

Der Name des Anforderungsprofils für ein Element ist eines seiner Attribute. Falls erforderlich, kann bei der Genehmigung der Registrierungsanforderung ein anderes Anforderungsprofil angegeben werden.

Funktion zur Sicherung und Wiederherstellung von Schlüsseln

Tivoli PKI stellt eine Funktion zur Verfügung, mit der die Sicherung und Wiederherstellung von Schlüsseln angefordert werden kann. Diese Funktion ermöglicht die Sicherung und Wiederherstellung von Endentitätszertifikaten und den zugehörigen privaten Schlüsseln, die von Tivoli PKI zertifiziert wurden.

Mit Hilfe dieser Funktion können verlorene, vergessene oder anderweitig abhanden gekommene Zertifikate und private Schlüssel wiederhergestellt werden. Betrachten Sie folgendes Szenario als Beispiel: Ein Angestellter führt routinemäßig eine Sicherung seiner Zertifikate und privaten Schlüssel aus und scheidet dann plötzlich aus der Firma aus, ohne alle privaten Schlüssel zurückzugeben, die für den Zugriff auf diese Informationen erforderlich sind. Durch Ausgabe einer Wiederherstellungsanforderung können Sie Informationen abrufen, die vormals verloren gewesen wären.

Im Allgemeinen umfasst der Sicherungsprozess die Erstellung einer PKCS #12-Datei durch den Benutzer. Diese Datei enthält das Zertifikat und den privaten Schlüssel des betreffenden Benutzers. Der Benutzer gibt über einen unterstützten Browser eine Sicherungsanforderung aus und verwendet dabei die PKCS #12-Datei als Eingabe. Die Datenbank 'krbdb' für die Wiederherstellung von Schlüsseln wird aktualisiert und enthält die entsprechenden Zugriffsinformationen. Die Wiederherstellung von Schlüsseln funktioniert auf ähnliche Weise: Zunächst wird eine Wiederherstellungsanforderung für die zuvor gesicherte PKCS #12-Datei ausgegeben. Nachdem die Anforderung vom RA-Administrator genehmigt wurde, wird die Datei zum Downloaden für Sie bereitgestellt.

5

Referenzinformationen

Die Themen in diesem Abschnitt umfassen Informationen zu Verzeichnisstrukturen, Feldbeschreibungen sowie zulässigen Werten und erläutern die Bedeutung von Attributen, die beim Anpassen der Registrierungsfunktion möglicherweise benötigt werden. Unter jeder Hauptüberschrift finden Sie die zugehörigen Unterthemen in alphabetischer Reihenfolge.

Anpassungs-Tools

Die folgenden Tools können zum Anpassen von Tivoli PKI eingesetzt werden.

Komponente	Dateityp	Anpassungs-Tool
Bildmaterialdateien	*.gif	Alle Grafikpakete, die das GIF-Format unterstützen.
Andere anpassbare Dateien	*.cfg *.jsp *.ltr *.txt	Alle Unicode-Editoren, die das Importieren und Exportieren von Daten im UTF-8-Format unterstützen. ■ Unter Windows NT können Sie den Editor UnicEdit verwenden, den Sie als Freewarekomponente mit Ihrem Browser herunterladen können. ■ Unter AIX können Sie das Tool 'iconv' verwenden.

Anmerkungen:

1. Vor der Durchführung von Änderungen an einer Datei sollten Sie immer eine Sicherungskopie erstellen.
2. Wenn Sie Tivoli PKI unter Windows NT installiert haben, müssen Sie allen für die Registrierungsfunktion erstellten Ressourcendateien (z. B. allen HTML- und JSP-Dateien) Namen in Kleinbuchstaben zuordnen. Verwenden Sie als Dateinamen z. B. 'my.html', jedoch nicht 'MY.html' oder 'My.html'. Andernfalls gibt der IBM HTTP-Server für alle Dateinamen, die Großbuchstaben oder Buchstaben in Groß-/Kleinschreibung enthalten, das Folgende zurück:

ERROR 404 NOT FOUND

Dieser HTTP-Server-Fehler tritt bei Installationen unter AIX nicht auf.

3. Bei Ländern, für die Nicht-ASCII-Zeichen erforderlich sind, werden Werte in Tivoli PKI-Anwendungsdateien im UTF-8-codierten Unicode-Format definiert. Unicode/UTF-8 erlaubt das universelle Codieren von Zeichen und ermöglicht Tivoli PKI die gleichzeitige Unterstützung mehrerer Sprachen auf dem selben System und sogar innerhalb eines Zertifikatsprofils. Wenn eine Datei UTF-8-codierte Daten enthält, muss beim Editieren mit besonderer Vorsicht vorgegangen werden, um die Beschädigung der UTF-8-Werte zu

verhindern. Sie können wie oben beschrieben einen Editor verwenden oder die Datei in eine native Codepage konvertieren, diese dann editieren und sie anschließend zurück in das UTF-8-Format konvertieren.

Dateiadressen

Dieser Abschnitt enthält die Namen und Adressen für Elemente, die Sie für Ihre Registrierungsdomäne anpassen können.

Verzeichnisstruktur

Während der Konfiguration werden die Dateien der Registrierungsfunktion in den Verzeichnispfad Ihrer Registrierungsdomäne kopiert. Im Folgenden ist die Standardverzeichnisstruktur dargestellt. Der Name Ihrer Domäne und der zugehörige Installationspfad können von den Standardwerten für die Tivoli PKI-Installation abweichen. Die korrekten Werte erfahren Sie beim zuständigen Systemadministrator.

Unter AIX:

/usr/lpp/iau/pkrf/Domains/YourDomain

Unter Windows:

c:\Program Files\IBM\Trust Authority\pkrf\Domains\YourDomain

Die folgenden Komponenten Ihrer Registrierungsfunktion sind bestimmten Anpassungs-Tasks zugeordnet oder stehen in enger Beziehung zu diesen.

Komponente	Unterverzeichnis	Dateiname
Zertifikatsprofile	etc	certificate_profiles.cfg
Anzeigenamen für Zertifikatstypen, Zertifikatsbeschreibungen	etc	*.txt
E-Mail-Benachrichtigungsbriefe	etc	*.ltr
Grafikdateien	Web-Seiten	*.gif
HTML-Dateien	Web-Seiten	*.html
Java Server-Seiten	Web-Seiten	*.jsp
Regel-Exit	bin	auto_approve.exe
Konfigurationsdatei der Registrierungsfunktion	etc	raconfig.cfg
Servlets kompilierter JSP-Dateien	.\servlets\pagecompile\YourDomain	

Anpassbare Elemente

In der folgenden Tabelle sind alle Elemente Ihrer Registrierungsfunktion aufgeführt, die Sie anpassen können. Darüber hinaus enthält sie Informationen dazu, in welcher Komponente das Element enthalten ist.

Anpassbares Element	Zu editierende Komponente
Bildmaterial auf JSP-Seiten	Java Server-Seiten
Banner auf einer Registrierungsseite	Java Server-Seiten
Bei der Registrierung für den Benutzer angezeigter Text	Zertifikatsprofile (certificate_profiles.cfg), Konfigurationsdatei der Registrierungsfunktion (raconfig.cfg)

Anpassbares Element	Zu editierende Komponente
Registrierungsfelder und Werte in Auswahllisten	Zertifikatsprofile (certificate_profiles.cfg), Konfigurationsdatei der Registrierungsfunktion (raconfig.cfg)
Namen von Zertifikatsangeboten	Zertifikatsprofile (certificate_profiles.cfg)
Beschreibungen von Zertifikatsangeboten	Java Server-Seite (CertTypes.jsp)
Merkmale der einzelnen Zertifikatstypen	Zertifikatsprofile (certificate_profiles.cfg)
Beispiel für eine E-Mail-Benachrichtigung zur Information über Genehmigung oder Zurückweisung einer Anforderung	E-Mail-Benachrichtigungsbrief
Regel-Exit zur Unterstützung der automatischen Genehmigungsverarbeitung	Regel-Exit
URL-Adresse, die dem Registrator beim Verlassen von RA Desktop angezeigt wird	RA Desktop-Java Server-Seite (radesktop.jsp)
Ablaufzeitraum für Registrierungsanforderungen	Zertifikatsprofile (certificate_profiles.cfg)
Erforderliche Felder im Registrierungsformular	Zertifikatsprofile (certificate_profiles.cfg)
Objektklassen für Verzeichniseinträge	Zertifikatsprofile (certificate_profiles.cfg)

Anmerkung: Nach dem Ändern eines Elementes müssen Sie möglicherweise noch kleinere Änderungen an anderen Dateien vornehmen, um Ihre Modifikationen zu implementieren. Informationen zu den für eine Anpassungs-Task erforderlichen Arbeitsschritten finden Sie in den Informationen zur Vorgehensweise.

Quellendateien auf den Webseiten

Dieses Thema enthält eine Liste der Java Server-Seiten, die als Quellendateien für die Registrierungs-Web-Seiten verwendet werden können. Die Namen dieser Quellendateien sind Komponenten der Webadressen, die bei der Durchführung der Registrierung für Ihre Registrierungsfunktion verwendet werden. Sie können unterschiedliche Webadressen angeben. Wenn Sie eigene Werte einsetzen, benennen Sie diese in der Konfigurationsdatei der Registrierungsfunktion um.

Wurde diese Einstellung in Ihrem Unternehmen nicht geändert, setzen sich Webadressen immer aus dem Namen Ihres öffentlichen Webservers und Ihrem Domänennamen zusammen. Lautet beispielsweise der Name Ihres öffentlichen Webservers 'MyPublicWebServer' und der Domänenname 'MyDomain', können Sie über die folgende Webadresse auf die Registrierungsfunktion zugreifen:

`http://MyPublicWebServer/MyDomain/`

Zu dieser Basiskomponente werden die folgenden JSP-Seiten hinzugefügt, um die Webadressen für die Registrierungswebseiten zu vervollständigen. Werden mehrere Dateien angezeigt, gelten die mit der Zeichenfolge "NS" beginnenden Namen für den Browser Netscape. Die Namen, die mit "IE" beginnen, können im Browser Internet Explorer angezeigt werden.

Seite	Zweck	Dateiname
Identitätsnachweis - Verwaltung	Homepage	index.jsp

Seite	Zweck	Dateiname
Registrierungsformulare für alle Registrierungstypen	Browser Netscape Browser Internet Explorer Server oder Einheiten Vorabregistrierung	NSBrowserSSLcert_Enroll.jsp IEBrowserSSLcert_Enroll.jsp PKCS107Cert_Enroll.jsp PreReg_Enroll.jsp
Beschreibungen von Zertifikaten	Anzeigenamen Beschreibungen	certificate_profiles.cfg CertTypes.jsp
Seiten für Benutzer-rückmeldungen	Fehlernachrichten Instruktionen nach dem Übergeben	TA_ErrorMsg.jsp *_CkStatus.jsp
Statusinformationen	Genehmigung Wartestatus Zurückweisung	*_Approved.jsp *_Pending.jsp *_Rejected.jsp
Erneuerungsformular für Browser-Zertifikate	Netscape Internet Explorer	NSBrowserSSLcert_Renew.jsp IEBrowserSSLcert_Renew.jsp
Zurückweisungsformular für Browser-Zertifikate	Netscape Internet Explorer	NSBrowserSSLcert_Revoke.jsp IEBrowserSSLcert_Revoke.jsp
Bestätigung für Widerrufanforderung	Netscape Internet Explorer	NSBrowserSSLcert_RevokeRecd.jsp IEBrowserSSLcert_RevokeRecd.jsp

Beispieldateien

Die folgenden Themen enthalten die Dateien bzw. Auszüge aus den Dateien, die von Ihnen angepasst werden können. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden. Darüber hinaus sollten Sie zuerst eine Sicherungskopie der Originaldateien erstellen. Wenn Sie Dateien umbenennen oder eigene Dateien für diese einsetzen, müssen Sie die Konfigurationsdatei der Registrierungsfunktion entsprechend ändern, damit die Modifikationen wirksam werden.

Beschreibungsdateien für Zertifikatstypen

Dateiname

CertTypes.jsp

Adresse

Web-Seiten-Unterverzeichnis für Ihre Registrierungsdomäne

Beispiel

Original:

```
; --- S S L B R O W S E R C E R T 1 Y E A R --- [SSLBrowserCert1Year]
display_name=Web Client Authentication (1-Year)
```

Ersetzen durch:

```
; --- S S L B R O W S E R C E R T 1 Y E A R --- [SSLBrowserCert1Year]
display_name=My certificate Profile (1-Year)
```

Konfigurationsdatei für Zertifikatsprofile

Die Konfigurationsdatei für Zertifikatsprofile enthält Profile für die Zertifikate, die in Ihrem Unternehmen zur Verfügung stehen.

- Der Registrator kann den Ablaufzeitraum für die Registrierungsanforderung feststellen. Hierbei handelt es sich um den Zeitraum, nach dem eine übergebene Registrierungsanforderung abläuft und kein Anforderungsstatus oder Identitätsnachweis mehr ausgegeben wird.
- Der Registrator kann die erforderlichen Felder feststellen, die der Endbenutzer auf dem Registrierungsformular ausfüllen muss.
- Ein Benutzer kann diese aus einer Liste auswählen, wenn er sich für einen bestimmten Zertifikatstyp entscheidet.

Sie können die in der Datei definierten Profile ändern oder ein Profil kopieren und als Schablone für das Erstellen zusätzlicher Zertifikatsangebote verwenden.

Dateiname

certificate_profiles.cfg

Adresse

Unterverzeichnis 'etc' für Ihre Registrierungsdomäne

Beispiele

- Ändern Sie den Anzeigenamen für ein Zertifikatsprofil.

Original:

```
; --- S / M I M E C e r t 1 Y e a r ---
[S/MIMECert1Year] display_name=E-mail Protection (1-Year)
required_fields=first_name,last_name,email_address
```

Ersetzen durch:

```
; --- S / M I M E C e r t 1 Y e a r ---
[S/MIMECert1Year] display_name=Secure E-mail (1-Year)
required_fields=first_name,last_name,email_address
```

- Fügen Sie den Ablaufzeitraum für die Registrierungsanforderung zu einem bestimmten Zertifikatsprofil hinzu.

```
; --- S / M I M E C e r t 1 Y e a r ---
[S/MIMECert1Year] display_name=E-mail Protection (1-Year)
required_fields=first_name,last_name,email_address
request_expires_in_hours=72
```

- Ändern Sie den Ablaufzeitraum für die Registrierungsanforderung bei allen Profilen.

Original:

```
request_expires_in_hours=72
```

Ersetzen durch:

```
request_expires_in_hours=48
```

- Ändern Sie die erforderlichen Felder für ein bestimmtes Zertifikatsprofil.

Original:

```
; --- S / M I M E C e r t 1 Y e a r --
[S/MIMECert1Year] display_name=E-mail Protection (1-Year)
required_fields=first_name,last_name,email_address
```

Ersetzen durch:

```
; --- S / M I M E C e r t 1 Y e a r --  
[S/MIMECert1Year] display_name=E-mail Protection (1-Year)  
required_fields=first_name,last_name,CN
```

- Ändern Sie die Standarddefinitionen der erforderlichen Felder in allen Profilen.

Original:

```
; --- Define field processing values  
displayable_fields=subjectName,issuerName,  
keyUsage,validityNotAfter,validityNotBefore  
editable_fields=subjectName,  
validityNotAfter,validityNotBefore  
required_fields=first_name,last_name
```

Ersetzen durch:

```
; --- Define field processing values  
displayable_fields=subjectName,issuerName,  
keyUsage,validityNotAfter,validityNotBefore  
editable_fields=subjectName,  
validityNotAfter,validityNotBefore  
required_fields=first_name,last_name,email_address
```

Speichern Sie vor dem Editieren eine Sicherungskopie der Originaldatei. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden. Wenn Sie die Datei umbenennen, müssen Sie auch den Namen ändern, der in der Konfigurationsdatei der Registrierungsfunktion definiert ist.

E-Mail-Benachrichtigungsbrief

Dieses Thema behandelt den E-Mail-Benachrichtigungsbrief für Ihre Registrierungsfunktion.

Dateiname

*.ltr

Adresse

Unterverzeichnis 'etc' für Ihre Registrierungsdomäne

Beispiel

Dieser Brief wird an Antragsteller gesendet, die nach der Verarbeitung ihrer Registrierungsanforderung eine E-Mail-Benachrichtigung anfordern.

Microsoft Internet Explorer Browser Certificate Enrollment Status

=====

This mail was sent by an automatic mail sender that
does not answer incoming mail. Please do not reply.

=====

To: %%first_name%% %%last_name%%
From: Trust Authority Certificate Enrollment

Request ID: %%RequestID%%

Your enrollment request for a Microsoft Internet Explorer browser
certificate has been finalized.

Please access the following URL from your browser, then follow the
online instructions to check your enrollment status.

%%UE_SERVER_AUTH_URL_PATH%%JSP_MOUNT_POINT%%Page_CkStatus_IEBrowserSSLCert%%?name=
%%URLEncodedCN%%&id=%%URLEncodedRequestID%%&cq=%%URLEncodedChallengeQ%%

Beachten Sie hierbei, dass der Code in den endgültigen Zeilen des obigen Beispiels in einer einzigen Zeile angegeben werden muss.

Die folgenden Ersetzungsvariablen stehen für die E-Mail-Benachrichtigungsschablone zur Verfügung und können an beliebiger Stelle im Hauptteil des Texts verwendet werden.

Variable	Beschreibung
first_name	Vorname
last_name	Nachname
RequestID	Anforderungsname
URLEncodedRequestID	URL-codierte Anforderungs-ID
action_comment	Kommentar zu der vom Registrator ausgeführten Aktion
domain	Domänenname
URLEncodedChallengeQ	URL-codierte Abfragenfrage
URLEncodedCN	URL-codierter allgemeiner Name (CN)

Anmerkungen:

1. Speichern Sie eine Sicherungskopie der Datei, bevor Sie das Original editieren.
2. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden.
3. Die erste Zeile im Benachrichtigungsbrief wird als Betreffzeile interpretiert.
4. Wenn Sie die Datei umbenennen oder eigene Dateien hinzufügen oder anstatt der Standarddateien verwenden, müssen Sie auch die Namen ändern, die in der Konfigurationsdatei der Registrierungsfunktion definiert sind.
5. Wenn das System, auf dem der RA-Server ausgeführt wird, nicht über einen SMTP-Server verfügt, definieren Sie einen Zeiger auf einen neuen Server. Fügen Sie hierzu ein Name/Wert-Paar in der Konfigurationsdatei der Registrierungsfunktion hinzu. Der Name des Eintrags ist MAIL_SMTP_HOST und der zugehörige Wert ist der Host-Name des Servers. Wenn Sie z. B. den Host-Namen 'mailserver.mycorp.com' definiert haben, müssen Sie folgenden Eintrag in der Datei 'raconfig.cfg' hinzufügen:

```
MAIL_SMTP_HOST=mailserver.mycorp.com
```

Fehlernachrichtentext

Sie können den Wortlaut von Fehlernachrichten ändern, um diese für die Benutzer Ihres Unternehmens verständlicher zu formulieren.

Dateiname

TA_ErrorMsg.jsp

Adresse

Web-Seiten-Unterverzeichnis für Ihre Registrierungsdomäne

Beispiel

Original:

```
STRING_ErrorMsg[3] = "An error occurred while your enrollment status was being retrieved. Check your enrollment status later to see if the problem has been resolved.";
```

Ersetzen durch:

```
STRING_ErrorMsg[3] = "Your enrollment status is not available at this time. Please check your enrollment status later or call (800) XXX-XXXX for further assistance.";
```

Java Server-Seite (JSP)

Die Java Server-Seiten (JSP-Dateien) umfassen ein Banner, Bildmaterial, Text und Formularfelder für die Registrierung.

Dateiname

*.jsp

Adresse

Web-Seiten-Unterverzeichnis für Ihre Registrierungsdomäne

Beispiel

Eine Java Server-Seite enthält HTML-Formatierungssteuerzeichen, Java-Scriptlets und möglicherweise auch JavaScripts.

HTML

```
<title>TrustAuthority Credential Enrollment</TITLE>
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<BODY TEXT="#000000" BGCOLOR="#FFFFFF" LINK="#006699" VLINK="#006699"
ALINK="#006699">
<P><CENTER>
<TABLE WIDTH="600" BORDER="0" CELSPACING="0">
```

JAVA

```
<%@ import = "java.io.*,java.util.*,javax.servlet.http.HttpUtils,java.net.*,
com.ibm.irg.ra.css.*,com.ibm.irg.ra.afw.approver.*" %>
// Obtain instance of Approver and create raconfig object.
try { Approver approver = ApproverFactory.getInstance( urlString );
    raConfig raconfig = approver.getRaConfig();
appDomain = approver.getApplicationDomain();
    Page_Enroll_NSBrowserSSLCert = raconfig.find( appDomain,
"Page_Enroll_NSBrowserSSLCert" );
} catch ( Exception e ) {
```

JavaScript

```
<SCRIPT LANGUAGE="JavaScript">
<!--
function ReplaceSubstring( theString, outString, inString ) {

    var index = 0;
    while ( ( index = theString.indexOf( outString, index ) ) >= 0 ) {
        theString = theString.substring( 0, index ) + inString +
            theString.substring( index + outString.length );
        index += inString.length;
    }
    return theString;
}
//-->
</SCRIPT>
```

Speichern Sie vor dem Editieren eine Sicherungskopie der Originaldatei. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden. Wenn Sie eine der Dateien umbenennen oder eigene Dateien hinzufügen oder anstatt der Standarddateien verwenden, müssen Sie die Namen in der Konfigurationsdatei der Registrierungsfunktion ändern.

Regel-Exit-Datei

Der Beispiel-Regel-Exit, der zum Lieferumfang der Registrierungsfunktion gehört (auto_approve.cpp), wird von Tivoli PKI-Geschäftsprozessen aufgerufen. Er dient zum Prüfen des Wertes der Variablen 'decision_default' und zur Ausführung entsprechender Aktionen.

Dateiname

auto_approve.cpp

Dieser Name wird in der Datei 'raconfig.cfg' definiert und im Eintrag 'afservice.PolicyExit' angegeben.

Adresse

Unterverzeichnis 'bin' für den Installationspfad Ihrer Registrierungsdomäne.

Beispiel

Die folgende Liste enthält relevante Codesegmente aus dem Beispielprogramm 'auto_approve'. Dieser Code zeigt, wie Regel-Exits zum Lesen von Nachrichten aus der Standardeingabeeinheit (STDIN), zum Ausführen von Aktionen auf der Basis des Nachrichteninhalts sowie zum anschließenden Formulieren einer Antwort verwendet werden können, die an die Tivoli PKI-Geschäftsprozesse zurückgegeben wird. Sie können an diesem Beispiel sehen, wie stark die Komplexität angepasster Regel-Exits zunehmen kann. Verwenden Sie diesen Code als Richtlinie und befolgen Sie die bereits erläuterten Konventionen für den Nachrichtenaustausch und die Ein-/Ausgabe, die für den Regel-Exit gelten.

Der Beispielcode dient zur Ausführung der folgenden Operationen:

1. Lesen von Daten aus der Standardeingabeeinheit (STDIN), bis ein Zeilenvorschubzeichen gefunden wird.
2. Interpretieren der Daten, die von den Tivoli PKI-Geschäftsprozessen gesendet wurden. Beachten Sie, dass das hier verwendete Objekt 'raMessage' die Komplexität der URL-Codierung sowie der Extraktion von Name-/Wert-Paaren aus den Nachrichtendaten ausgleicht.
3. Extrahieren von Registrierungsinformationen (request_vars) und Geschäftsprozessinformationen (bp_vars) für die anschließende Verwendung in angepassten Logikkomponenten, die zu dem Regel-Exit hinzugefügt wurden, und Formulieren einer Antwortnachricht auf der Basis des Inhalts der Eingabenachricht.
4. Schreiben der Daten der Antwortnachricht in die Standardausgabereinheit (STDOUT) und Beenden der Antwort durch ein Zeilenvorschubzeichen. (Die Schreiboperationen wird hierbei wieder mit dem Objekt 'raMessage' durchgeführt.)

```

#include "ramsg.hpp"

void main (int argc, char *argv[])
{
    char message[64*1024];

    // Read message(s) from stdin
    while ( cin.good() )
    {
        message[0] = NULL;
        cin.getline(message,sizeof(message));

        // if message is not good or is a shutdown, we're done!
        if ( !cin.good() ) break;
        if ( strstr(message,"<<<<shutdown>>>") ) break;

        // create an raMessage object
        raMessage inmsg(message);

        // extract enrollment information (request_vars)
        raMessage reqvars(inmsg.findVariable("request_vars"));

        // extract business process information (bp_vars)
        raMessage bpvars(inmsg.findVariable("bp_vars"));

        // extract any other expected fields
        const char* bpname = inmsg.findVariable("RaBPName");
        const char* pearg = inmsg.findVariable("RaPolicyExitArg");
        const char* domain = inmsg.findVariable("domain");
        const char* decision_default = bpvars.findVariable("decision_default");

        // construct the response message object
        raMessage response(inmsg);
        response.erase();

        // Examine decision_default to determine what action should be taken
        // and formulate response message accordingly
        if ( strstr(decision_default, "approve") )
        {
            // insert custom business logic here
            response.addVariable("reqStatus", "Approved");
        }
        else if ( strstr(decision_default, "pend") )
        {
            // insert custom business logic here
            response.addVariable("reqStatus", "Pending");
        }
        else if ( strstr(decision_default, "revoke") )
        {
            // insert custom business logic here
            response.addVariable("ffStatus", "Revoked");
        }
        else if ( strstr(decision_default, "reject") )
        {
            // insert custom business logic here
            response.addVariable("reqStatus", "Rejected");
        }
        else
        {
            // insert custom business logic here
        }

        // send response
        response.streamObject(cout);
        cout <<<< endl;
    }
}

```

Konfigurationsdatei für die Registrierungsfunktion

Die Konfigurationsdatei der Registrierungsfunktion enthält Werte, die nach der Installation zur Benennung und Definition der Komponenten und Betriebseinstellungen für die folgenden Elemente angegeben werden:

- Debug-Stufe
- Zugriffseintrag für die Registrierungsdatenbank
- URL-Adressen des öffentlichen und gesicherten Web-Servers
- Mount-Punkte
- Dateinamen für Java Server-Seiten
- Dateiname für E-Mail-Benachrichtigungsbrief
- Name der Konfigurationsdatei für Zertifikatsprofile
- Vektorspezifische Zertifikatsprofile
- Name des Zertifikatsausstellers (CA)
- Verzeichnisname (Directory)
- RA-Server-Parameter
- Kommentare für die Aktionstabellen des RA-Servers
- Name der Konfigurationsdatei für RA Desktop
- RA Desktop-Webadresse
- Name der Schablonendatei für Geschäftsprozesse
- Approver Framework-Services und -Parameter

Dateiname

raconfig.cfg

Adresse

Unterverzeichnis 'etc' für Ihre Registrierungsdomäne

Speichern Sie vor dem Editieren eine Sicherungskopie der Originaldatei. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden. Wenn Sie die Datei umbenennen oder eigene Dateien anstatt der Standarddateien verwenden, müssen Sie auch den Namen ändern, der in der Konfigurationsdatei der Registrierungsfunktion definiert ist.

Die folgenden Unterabschnitte enthalten Auszüge aus der Datei, die in der Reihenfolge dargestellt sind, in der sie in der Datei definiert wurden.

Debug-Stufe

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
DebugLevel=0
```

Zugriffseintrag für Registrierungsdatenbank

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
RADATABASE= xxx
```

Dieser Wert ist verschlüsselt.

URL-Adressen des öffentlichen und gesicherten Web-Servers

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
PUBLIC_SERVER_URL_PATH=http://PublicWebServer/YourDomain/  
UE_SERVER_AUTH_URL_PATH=https://ServerAuthWebServer/YourDomain/  
UE_CLIENT_AUTH_URL_PATH=https://ClientAuthWebServer:1443/YourDomain/
```

Mount-Punkte

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
SERVLET_MOUNT_POINT=servlet/  
JSP_MOUNT_POINT=
```

Dateinamen für Java Server-Seiten (JSP)

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

Allgemeine Java Server-Seiten:

```
Page_Home=index.jsp  
Page_ErrorMsg=TA_ErrorMsg.jsp
```

Java Server-Seiten unter Netscape Navigator oder Netscape Communicator:

```
Page_Enroll_NSBrowserSSLCert=NSBrowserSSLCert_Enroll.jsp  
Page_CkStatus_NSBrowserSSLCert=NSBrowserSSLCert_CkStatus.jsp  
Page_Approved_NSBrowserSSLCert=NSBrowserSSLCert_Approved.jsp  
Page_Pending_NSBrowserSSLCert=NSBrowserSSLCert_Pending.jsp  
Page_Rejected_NSBrowserSSLCert=NSBrowserSSLCert_Rejected.jsp  
Page_Renew_NSBrowserSSLCert=NSBrowserSSLCert_Renew.jsp  
Page_Revoke_NSBrowserSSLCert=NSBrowserSSLCert_Revoke.jsp  
Page_RevokeRecd_NSBrowserSSLCert=NSBrowserSSLCert_RevokeRecd.jsp
```

Java Server-Seiten unter Microsoft Internet Explorer:

```
Page_Enroll_IEBrowserSSLCert=IEBrowserSSLCert_Enroll.jsp  
Page_CkStatus_IEBrowserSSLCert=IEBrowserSSLCert_CkStatus.jsp  
Page_Approved_IEBrowserSSLCert=IEBrowserSSLCert_Approved.jsp  
Page_Pending_IEBrowserSSLCert=IEBrowserSSLCert_Pending.jsp  
Page_Rejected_IEBrowserSSLCert=IEBrowserSSLCert_Rejected.jsp  
Page_Renew_IEBrowserSSLCert=IEBrowserSSLCert_Renew.jsp  
Page_Revoke_IEBrowserSSLCert=IEBrowserSSLCert_Revoke.jsp  
Page_RevokeRecd_IEBrowserSSLCert=IEBrowserSSLCert_RevokeRecd.jsp
```

Java Server-Seiten für Serverzertifikate:

```
Page_Enroll_PKCS107Cert=PKCS107Cert_Enroll.jsp  
Page_CkStatus_PKCS107Cert=PKCS107Cert_CkStatus.jsp  
Page_Approved_PKCS107Cert=PKCS107Cert_Approved.jsp  
Page_Pending_PKCS107Cert=PKCS107Cert_Pending.jsp  
Page_Rejected_PKCS107Cert=PKCS107Cert_Rejected.jsp  
Page_Sample_PKCS107Cert=PKCS107Cert_Sample.jsp
```

Java Server-Seiten für Vorabregistrierung von Zertifikaten:

```
Page_Enroll_PreReg=PreReg_Enroll.jsp  
Page_CkStatus_PreReg=PreReg_CkStatus.jsp  
Page_Approved_PreReg=PreReg_Approved.jsp  
Page_Pending_PreReg=PreReg_Pending.jsp
```

Dateiname für E-Mail-Benachrichtigungsbrief

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

Für Windows:

```
Mail_Template_NSBrowserSSLCert=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\
Mail_Template_NSBrowserSSLCert.ltr
Mail_Template_IEBrowserSSLCert=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\
Mail_Template_IEBrowserSSLCert.ltr
Mail_Template_PKCS107Cert=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\
Mail_Template_PKCS107Cert.ltr
Mail_Template_PreReg=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\
Mail_Template_PreReg.ltr
```

Für AIX:

```
Mail_Template_NSBrowserSSLCert=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/
Mail_Template_NSBrowserSSLCert.ltr
Mail_Template_IEBrowserSSLCert=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/
Mail_Template_IEBrowserSSLCert.ltr
Mail_Template_PKCS107Cert=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/
Mail_Template_PKCS107Cert.ltr
Mail_Template_PreReg=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/
Mail_Template_PreReg.ltr
```

Name der Konfigurationsdatei für Zertifikatsprofile

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

Für Windows:

```
CertificateProfiles=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\
certificate_profiles.cfg
```

Für AIX:

```
CertificateProfiles=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/certificate_profiles.cfg
```

Vektorspezifische Zertifikatsprofile

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
CertProfiles_NSBrowserSSLCert=SSLBrowserCert1Year,SSLBrowserCert2Year,S/MIMECert1Year,
S/MIMECert2Year
CertProfiles_IEBrowserSSLCert=SSLBrowserCert1Year,SSLBrowserCert2Year,S/MIMECert1Year,
S/MIMECert2Year
CertProfiles_PKCS107Cert=SSLServerCert1Year,SSLServerCert2Year,IPSecCert1Year,IPSecCert2Year
CertProfiles_PreReg=S/MIMECert1Year,S/MIMECert2Year,IPSecCert1Year,IPSecCert2Year,
SSLServerCert1Year,SSLServerCert2Year,SSLBrowserCert1Year,SSLBrowserCert2Year,
SignatureOnlyCert1Year,SignatureOnlyCert2Year,KeyEnciphermentCert1Year,
KeyEnciphermentCert2Year,DataEnciphermentCert1Year,DataEnciphermentCert2Year,
NonRepudiationCert1Year,NonRepudiationCert2Year,CACrossCertificationRequest
```

Name des Zertifikatsausstellers (CA)

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie weicht in der von Ihnen verwendeten Datei voraussichtlich vom u. a. Format ab:

```
issuerName_webserver=/C=US/O=Your Organization/OU=Trust Authority/CN=Trust Authority CA
```

Verzeichnisname (Directory)

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
issuerDirectory_webserver=ldap://DirectoryServer:389
```

RA Server-Parameter

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
PKIX_RA_URL=pkix://RAServer:829
RASD_URL=rasd://RAServer:29783
RASDThreadCount=25
RASDPendingTimeout=360
RASDJNHRecycleCount=100000
raserver_name=raserver
```

Für Windows:

```
RASDJNHIni=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\jonahra.ini
```

Für AIX:

```
RASDJNHIni=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/jonahra.ini
```

Kommentare für RA Server-Aktionstabelle

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
pkix_prereg_info_added_to_db=PKIX Preregistration info added to database
certificate_added_to_db=Certificate added to the database
ca_rejected_cert_request=CA rejected certificate request
certificate_revoked_by_ca=Certificate Revocation Completed by CA
error_info_added_to_db=Error information added to the database
ca_rev_rej_reason_added_to_db=CA's revocation rejection reason added to the database
cert_confirmed_updated_in_db=Certificate "delivery confirmed" status updated in the database
cert_delivered_updated_in_db=Certificate delivered confirmation status updated in the database
jnh_request_id_added_to_db=Jonah request identifier added to the database
```

Name der RA Desktop-Konfigurationsdatei

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

Für Windows:

```
raprofiles=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\raprofiles.cfg
```

Für AIX:

```
raprofiles=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/raprofiles.cfg
```

URL-Adresse für RA Desktop

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
RAD_CLIENT_AUTH_URL_PATH=https://ClientAuthWebServer:1443/YourDomain/
```

Name der Schablonendatei für Geschäftsprozesse

Das folgende Beispiel zeigt die Standardzeile für diese Angabe. Sie sollte in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

Für Windows:

```
bptemplatefile=C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\etc\BPTemplates.txt
```

Für AIX:

```
bptemplatefile=/usr/lpp/iau/pkrf/Domains/YourDomain/etc/BPTemplates.txt
```

Approver Framework-Services und -Parameter

Das folgende Beispiel zeigt die Standardzeilen für diese Angabe. Sie sollten in der von Ihnen verwendeten Datei das u. a. Format aufweisen:

```
TokenTimeout=12
afservice.trace=com.ibm.irg.ra.afw.services.TraceSyserrSvcFactory,ShowElapsed=true
afservice.RASD=com.ibm.irg.ra.afw.services.CallRASDviaSocketSvcFactory
queued_bp_processor_threads=10
afw_bpo_caching=true
ldap_autoCreate_entries=false // this variable is boolean true or false
afservice.LdapPolicy=com.ibm.irg.ra.afw.services.LDAPPolicyServiceFactory,
PolicyClass=com.ibm.irg.ra.efw.bpos.LDAPSampleCreationPolicy
```

Für Windows:

```
afservice.RADB=com.ibm.irg.ra.afw.services.RaReqDatabaseServiceFactory,
com.ibm.irg.ra.css.raReqDatabaseProxyLocalAgent,cfguser,
pkrfdb,,,cfguser,language=en,codepage=UTF-8,reqdbagent=C:\PROGRA~1\IBM\TRUSTA~1\
bin\reqdbagent
afservice.PolicyExit=com.ibm.irg.ra.afw.services.SpawnPolicyExitLongRunningFactory,
C:\PROGRA~1\IBM\TRUSTA~1\pkrf\Domains\YourDomain\bin\auto_approve
afservice.audit=com.ibm.irg.ra.afw.services.CallAuditviaSocketSvcFactory,C:\PROGRA~1\IBM\
TRUSTA~1\etc\AuditClient.ini
```

Für AIX:

```
afservice.RADB=com.ibm.irg.ra.afw.services.RaReqDatabaseServiceFactory,
com.ibm.irg.ra.css.raReqDatabaseProxyLocalAgent,cfguser,
pkrfdb,,,cfguser,language=en,codepage=UTF-8,reqdbagent=/usr/lpp/iau/bin/reqdbagent
afservice.PolicyExit=com.ibm.irg.ra.afw.services.SpawnPolicyExitLongRunningFactory,
/usr/lpp/iau/pkrf/Domains/YourDomain/bin/auto_approve
afservice.audit=com.ibm.irg.ra.afw.services.CallAuditviaSocketSvcFactory,
/usr/lpp/iau/etc/AuditClient.ini
```

Einzelangaben auf den Webseiten

Dieser Abschnitt enthält Referenzinformationen für die Anpassung von Elementen auf Registrierungs-Web-Seiten.

Registrierungsformularvariablen

Das Registrierungsformular auf den Java Server-Seiten verfügt über Abschnitte zum Beschreiben des zukünftigen Zertifikatseigners und der Zertifikatsanforderung. Bestimmte Felder in den Abschnitten werden nur bei speziellen Registrierungstypen angezeigt.

Im vorliegenden Abschnitt werden die Formularvariablen für die Registrierung aufgelistet und beschrieben. Sie befinden sich auf den Java Server-Seiten. In den folgenden Tabellen werden die Formularfelder den zugehörigen Formularvariablen zugeordnet. Sie können diese verwenden, wenn Sie Informationen zum Registrierungsprozess erfassen müssen.

Dateiname

*._Enroll.jsp

Adresse

Web-Seiten-Unterverzeichnis für Ihre Registrierungsdomäne

Felder für Registrierungsinformationen

Anmerkungen:

1. Feldwerte sind - sofern nichts anderes angegeben wurde - optional und werden in allen Registrierungsformularen verwendet.
2. Längenangaben definieren die maximal zulässige Anzahl von Zeichen. Wird keine Längenangabe aufgeführt, handelt es sich bei dem Feld um ein Markierungsfeld oder eine Auswahlliste.
3. Andere Einschränkungen betreffen erforderliche Felder und ungültige Zeichen für bestimmte Feldwerte, die zu einem registrierten Namen (DN) zusammengefasst werden.
4. Die Tabelle enthält keine internen Formularvariablen für Internet Explorer, die nicht an den Server gesendet werden. Diese werden lediglich zum Generieren der PKCS #10-Anforderung verwendet.

Feldname	Anzeigename	Länge	Inhalt
certificate_profile	Zertifikatstyp	Beliebig	(Erforderlich) Der Zertifikatstyp. Informationen zu den bei einer Standardinstallation bereitgestellten Zertifikatstypen finden Sie in „Zertifikatstypen“ auf Seite 62. Das Formular enthält eine Liste der geeigneten Zertifikatstypen für den gewünschten Registrierungstyp.
first_name	Vorname	31	(Erforderlich) Der Vor- oder Taufname des Zertifikatsantragstellers. Der Antragsteller kann bei Bedarf einen zweiten Vornamen oder dessen Initiale angeben. Bei der Vorabregistrierung bezieht sich diese Angabe auf die Person oder Entität, für die die Vorabregistrierung durchgeführt wird.
last_name	Nachname	32	(Erforderlich) Der Nach- oder Familienname des Antragstellers. Bei der Vorabregistrierung bezieht sich diese Angabe auf die Person oder Entität, für die die Vorabregistrierung durchgeführt wird.
email_address	E-Mail-Adresse	128	Die E-Mail-Adresse des Antragstellers einschließlich des Zeichens @ und aller Punkte (.). Bei bestimmten Zertifikatstypen (z. B. Zertifikaten für gesicherte E-Mail-Übertragungen) wird diese Adresse benötigt. Wenn Sie die Option für die E-Mail-Benachrichtigung auswählen, muss der Antragsteller eine E-Mail-Adresse angeben.
decision_notification	E-Mail-Benachrichtigung		Eine Option zum Empfangen einer E-Mail-Benachrichtigung zum Status der aktuellen Registrierungsanforderung. Die Benachrichtigung wird an die im Formular angegebene E-Mail-Adresse gesendet.
challenge_q	Abfragefrage	48	Eine Frage, die sich speziell an den Antragsteller richtet und dazu dient, diesen zu authentifizieren. Dem Antragsteller wird diese Frage gestellt, wenn er den Status seiner Registrierungsanforderung prüfen will. Unabhängig davon, ob der Antragsteller sich selbst, einen Server oder eine andere Einheit registrieren lassen will oder eine Vorabregistrierung durchführt, muss er auf diese Frage antworten.
challenge_r	Abfrageantwort	48	(Groß-/Kleinschreibung beachten) Eine Antwort auf die Abfragefrage. Der Antragsteller muss die selbe Antwort geben, wenn er den Status seiner Anforderung prüfen will.

Feldname	Anzeigename	Länge	Inhalt
password	Kennwort	32	(Nur für die Vorabregistrierung) Das Kennwort, das die Person, für die die Vorabregistrierung durchgeführt werden soll, in der Client-Anwendung angeben muss, wenn alle vorbereitenden Maßnahmen für das Herunterladen des Zertifikats abgeschlossen sind. Das Kennwort muss zwischen 8 und 32 Zeichen lang sein und kann die Zeichen A - Z, a - z sowie die Ziffern 0 - 9 enthalten. Gibt der Antragsteller kein Kennwort an, generiert die Registrierungsfunktion ein aus zehn Zeichen bestehendes Kennwort. Bei Genehmigung der Vorabregistrierungsanforderung wird dieses zusammen mit einer Transaktions-ID an den Antragsteller gesendet.
confirmed_password	Kennwort bestätigen	32	(Nur für die Vorabregistrierung) Das identische Kennwort wird nochmals eingegeben.

Felder für die Zertifikatsanforderung

Anmerkungen:

1. Feldwerte sind - sofern nichts anderes angegeben wurde - optional und werden in allen Registrierungsformularen verwendet.
2. Längenangaben definieren die maximal zulässige Anzahl von Zeichen. Wird keine Längenangabe aufgeführt, handelt es sich bei dem Feld um ein Markierungsfeld oder eine Auswahlliste.
3. Andere Einschränkungen betreffen erforderliche Felder und ungültige Zeichen für bestimmte Feldwerte, die zu einem registrierten Namen (DN) zusammengefasst werden.
4. Die Tabelle enthält keine internen Formularvariablen für Internet Explorer, die nicht an den Server gesendet werden. Diese werden lediglich zum Generieren der PKCS #10-Anforderung verwendet.

Formularfeld	Anzeigename	Länge	Inhalt
pkcs10	PKCS #10-Zertifikatsanforderung		(Nur bei der Server- oder Einheitenregistrierung; Erforderlich) Der Inhalt der PKCS #10-Zertifikatsanforderung, die von den Servern bzw. Einheiten generiert wurde, für die der Antragsteller eine Registrierung durchführt. (Für Internet Explorer-Browser wird diese Anforderung automatisch generiert.)
CN	Allgemeiner Name	64	(Erforderlich) Ein Name zur Identifizierung des aktuellen Zertifikats. ■ Bei Personen wird hier normalerweise der vollständige Name angegeben. ■ Bei einem Server oder einer anderen Einheit wird normalerweise der Host-Name angegeben. Der Antragsteller muss diesen Wert angeben, wenn im Feld für die PKCS #10-Zertifikatsanforderung kein Host-Name definiert wurde.
nspk	Schlüsselgröße		(Nur bei der Netscape-Browser-Registrierung; Erforderlich) Die ausgewählte Schlüsselgröße für das Paar aus öffentlichem und privatem Schlüssel, das von Netscape generiert wird.
CSP	Verschlüsselungsserviceanbieter		(Nur bei der Internet Explorer-Browser-Registrierung; Erforderlich) Der Verschlüsselungsserviceanbieter, der das Paar aus öffentlichem und privatem Schlüssel generiert. Der Antragsteller kann hier einen Wert auswählen. ■ MBCP (Microsoft Base Cryptographic Provider) unterstützt die 512-Bit-Verschlüsselung von Schlüsseln. Dies ist der Standardwert. ■ MECP (Microsoft Enhanced Cryptographic Provider) unterstützt die 1024-Bit-Verschlüsselung von Schlüsseln.
KeyContainerName	Schlüsselsatz		(Nur bei der Internet Explorer-Browser-Registrierung) Das zu verwendende Schlüsselpaar. Der Antragsteller kann die Option Neuen Schlüsselsatz generieren auswählen oder die Liste öffnen und eines der vorhandenen Schlüsselpaare auswählen.
NewKeyName	Name des neuen Schlüsselsatzes		(Nur bei der Internet Explorer-Browser-Registrierung) Der Name für das neue Schlüsselpaar, das generiert werden soll. Der Antragsteller kann dieses Feld leer lassen und für den Namen eine GUID (Globally Unique Identifier) generieren lassen. Hierdurch ist das Schlüsselpaar jedoch schwieriger zu identifizieren.

Formularfeld	Anzeigenname	Länge	Inhalt
NewKeyAddedSecurity	Zusätzliche Sicherheitsoptionen		Zusätzliche Sicherheitsfunktionen, die Microsoft Internet Explorer für neue Schlüsselpaare unterstützt. Wenn der Antragsteller diese Option auswählt, zeigt der Web-Browser Internet Explorer-Dialoge zum Definieren dieser Optionen an, sobald ein Antragsteller dieses Registrierungsformular übergibt.
O	Firmenname	64	Der rechtlich registrierte Name des Unternehmens des Antragstellers.
OU	Abteilung	64	Der Name des Bereichs bzw. der Abteilung, in dem/der der Antragsteller tätig ist, z. B. Personalwesen oder Softwareentwicklung.
STREET	Straße	180	Die Straße, in der sich das Unternehmen des Antragstellers befindet.
L	Ort	128	Die Stadt oder Gemeinde, in der sich das Unternehmen des Antragstellers befindet, z. B. Chicago oder Paris.
ST	Bundesland	128	Das Bundesland, in dem sich das Unternehmen des Antragstellers befindet. Ihr Unternehmen und die Art und Weise, in der die Registrierungsfunktion dort eingesetzt wird, bestimmt, ob eine Standardabkürzung akzeptiert wird oder der vollständige Name angegeben werden muss. Sie können z. B. entweder New York oder NY verwenden.
C	Land/Verwaltungsbezirk	2	Das Land bzw. der Verwaltungsbezirk, in dem sich das Unternehmen des Antragstellers befindet. Hier wird eine Auswahlliste angezeigt.
domain_name	Domänenname	128	(Erforderlich für die Einheitenregistrierung) Der Host-Name der Maschine, auf der das angeforderte Zertifikat installiert werden soll. Andere Antragsteller geben diesen Wert nur dann an, wenn sie hierzu aufgefordert werden. Beispiel: mypc.mydiv.mycorp.com.
request_handler	(Keiner)		(Erforderlich) Die Java-Klasse, die zur Verarbeitung der Anforderung eingesetzt wird.

Widerrufsgründe

Wenn ein Benutzer, ein Registrator oder ein Regel-Exit ein Zertifikat widerruft, muss der hierfür geltende Grund angegeben werden. Im Folgenden sind gültige Gründe für das Widerrufen eines Zertifikats aufgeführt. Die Gründe sind auch auf den Java Server-Seiten definiert.

Der CA-Schlüssel war beschädigt

Der Schlüssel des Zertifikatsausstellers wurde beschädigt.

Das Zertifikat wurde ersetzt

Der Benutzer verfügt über ein neues Zertifikat und benötigt das vorliegende Zertifikat nicht mehr.

Keine Begründung

Der Benutzer hat den Widerruf ohne Angabe eines Grundes angefordert.

Der ursprüngliche Verwendungszweck ist nicht mehr gültig

Der Zertifikatseigner benötigt das Zertifikat nicht mehr für seine ursprüngliche Verwendung.

Benutzer hat die Zugehörigkeit geändert

Der Benutzer verfügt nicht mehr über die Zugehörigkeit, für die das Zertifikat angefordert wurde.

Der Benutzerschlüssel war beschädigt

Der private Schlüssel des Benutzers wurde beschädigt.

Einzeldaten von Zertifikaten

Im vorliegenden Abschnitt werden die Elemente aufgelistet und beschrieben, die zu einem Zertifikat gehören.

Zertifikatstypen

Ein Tivoli PKI-System stellt mehrere Zertifikatstypen für die unterstützten Zertifikatskategorien und Protokolle zur Verfügung.

- Der Registrator kann ein Profil aus einer Liste mit Anforderungsprofilen auf dem RA Desktop zuordnen.
- Ein Benutzer kann diese aus einer Liste auswählen, wenn er sich für einen bestimmten Zertifikatstyp entscheidet.

Der Name des Zertifikats zeigt an, wie lange es gültig ist und welche primäre Verwendung für den Schlüssel definiert wurde. Beschreibungen verschiedener Funktionen finden Sie im Glossar. Profile unterscheiden sich in den folgenden Punkten:

- Schlüsselverwendung (hierbei kann mehr als eine Funktion definiert werden)
- Gültigkeitszeitraum
- Möglicherweise hinzugefügte, benutzerdefinierte Erweiterungen

Sie können ein Profil kopieren und als Schablone für das Erstellen zusätzlicher Zertifikatsangebote für Ihr Unternehmen verwenden. Speichern Sie vor dem Editieren eine Sicherungskopie der Originaldatei. Die Änderungen können mit einem UTF-8-fähigen Texteditor vorgenommen werden. Wenn Sie ein Profil umbenennen oder eigene Profile hinzufügen oder anstatt der Standardprofile verwenden, müssen Sie die Namen in der Konfigurationsdatei der Registrierungsfunktion ändern, um diese Änderungen wirksam zu machen.

Zertifikatsprofile werden in einer Konfigurationsdatei für Zertifikatsprofile gespeichert.

Dateiname

certificate_profiles.cfg

Adresse

Unterverzeichnis 'etc' für Ihre Registrierungsdomäne

Dateiinhalte

```
Configuration File Structure
Global definitions
CA name
LDAP Directory name
keyUsage values (allow, default, priority)
validityNotBefore, validityNotAfter
subjectName components (C,O,OU,etc)
Stanza-specific definitions
[S/MIMECert1Year] CA Name
LDAP Directory Name
display_name=S/MIME Certificate - 1 year
validityNotAfter_range=0,365
validityNotAfter_default=365
Three ways of certificate extension definition:
form variables, pkcs10
certificate profile
policy exit
```

Bereitgestellte Profile

Antragsteller oder Personen, die für andere Personen eine Vorabregistrierung durchführen, können einen passenden Zertifikatstyp anfordern. Die einem Antragsteller zur Verfügung stehende Liste hängt von der Art der durchzuführenden Registrierung ab. Die Liste, die für Registratoren bereitgestellt wird, richtet sich nach den Berechtigungen, über die der Registrator in der Registrierungsdomäne verfügt.

Gegenseitig ausgestelltes CA-Zertifikat

Mit diesem Zertifikat kann der Zertifikatsaussteller (CA), dem dieses Zertifikat gehört, seine Zertifikate vom ausstellenden CA genehmigen lassen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Unbestreitbarkeit zur Verfügung.

1 und 2 Jahre - Datenverschlüsselung

Dieses Zertifikat ermöglicht dem Eigner die Verschlüsselung von Daten. Das Zertifikat dient keinem anderen Zweck.

1 und 2 Jahre - E-Mail-Schutz

Dieses Zertifikat ermöglicht dem Eigner die Verwendung des S/MIME-Protokolls (S/MIME = Secure Multi-Purpose Internet Mail Exchange). Dieses Protokoll dient zum Schutz von E-Mails und anderen MIME-Objekten. Es unterstützt die Authentifizierung des Absenders, die Integrität von Nachrichten, die Unbestreitbarkeit des Absenders sowie die Vertraulichkeit und wird normalerweise für Endbenutzer verwendet.

1 und 2 Jahre - IPSec

Dieses Zertifikat hilft bei der Gewährleistung der Integrität und Vertraulichkeit von Daten, die in IP-Paketen über das Internet versendet werden. IPSec-Zertifikate sind eher für Daten als für Benutzer gedacht. Sie sind häufig einem Router zugeordnet.

1 und 2 Jahre - Nur für Schlüsselcodierung

Dieses Zertifikat ermöglicht dem Eigner die Verschlüsselung von Schlüsseln. Das Zertifikat dient keinem anderen Zweck.

1 und 2 Jahre - Unbestreitbarkeit

Dieses Zertifikat stellt die Funktionen für Nachrichtenverschlüsselung und digitale Unterschriften zur Verfügung, um die Unbestreitbarkeit des Nachrichtenabsenders bzw. die Unbestreitbarkeit der Nachrichtenzustellung zu gewährleisten.

1 und 2 Jahre - Nur Unterschrift

Mit diesem Zertifikat kann der Eigner Dateien digital unterzeichnen. Das Zertifikat dient keinem anderen Zweck.

1 und 2 Jahre - Web-Client-Authentifizierung

Mit diesem Zertifikat kann ein Webbrowser an einer vom Client authentifizierten SSL-Sitzung teilnehmen. Der Benutzer des Browsers kann mit diesem Zertifikat auf eine bestimmte gesicherte Website zugreifen. Das Zertifikat stellt die Funktionen für digitale Unterschriften, Unbestreitbarkeit und Verschlüsselung von Schlüsseln zur Verfügung und wird normalerweise für Endbenutzer verwendet.

1 und 2 Jahre - Web-Server-Authentifizierung

Mit diesem Zertifikat kann ein Server an einer vom Server authentifizierten SSL-Sitzung teilnehmen. Das Zertifikat stellt die Funktionen für digitale Unterschriften und Verschlüsselung von Schlüsseln zur Verfügung.

Benutzerdefinierte Erweiterungen

Erweiterungen werden einem Zertifikat in Form von *Name-/Wert*-Paaren (*name=value*) hinzugefügt und können zu den Attributen gehören, die RA Desktop für ein Zertifikat anzeigt. Die folgenden Zertifikatserweiterungen sind für die Zertifikate von Personen zulässig, die eine gesicherte Anwendung benutzen wollen:

- Basiseinschränkungen
- Schlüsselverwendung
- Namenseinschränkungen
- Verwendungszeitraum für private Schlüssel
- Alternativname des Zertifikatsgegenstands

Format von X.509v3-Zertifikaten

Das Format eines X.509v3-Zertifikats wird von den meisten Verschlüsselungsprotokollen (einschließlich SSL) unterstützt. Die neuesten Informationen zu diesem Thema finden Sie auf der IETF-Website in den folgenden Dokumenten:

- *RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile* - Standard für Zertifikatsprofile und CRL-Profile einschließlich Zertifikatserweiterungen
- RFCs mit Beschreibungen anderer Standards für X.509v3-Zertifikate

Kopien dieser Dokumente können Sie über FTP abrufen. Beispiel:

FTP://ds.internic.net/rfc/rfc2459.txt

Einzelangaben bei der Registrierung

Die Themen in diesem Abschnitt definieren verschiedene Typen von Registrierungsdaten, die Sie möglicherweise bei eigenen Regel-Exits verwenden wollen.

Attribute von Anforderungen und Zertifikaten

Die folgenden Attribute werden im Datenbanksatz einer Registrierungsanforderung als **Anforderungsattribute** eingestuft:

Geschäftsprozessvariablen

Werte, die von einem Unternehmen während des Registrierungsprozesses angegeben werden. In diesem Attribut werden Gründe für den Widerruf eines Zertifikats bereitgestellt.

Ablaufdatum des Identitätsnachweises

Das Datum, an dem die Gültigkeit des Zertifikats abläuft.

Status 'Erneuerbar' des Identitätsnachweises

Gibt an, ob das Zertifikat erneuert werden kann.

Identitätsnachweis-UUID

Die UUID (Universal Unique Identifier = allgemeine, eindeutige Identitätsnachweis-ID) ist ein Primärschlüssel, der generiert wird, um einen Index für den Datenbanksatz bereitzustellen.

Fehlercode

Ein interner Code zur Kennzeichnung der Art des aufgetretenen Fehlers. Dieses Feld und das Feld **Fehlerursache** beschreiben den gleichen Fehler.

Fehlerursache

Der Prozess oder ein anderes Element von Tivoli PKI, in dem während der Verarbeitung von RA Desktop-Anforderungen ein Fehler aufgetreten ist.

Vorname

Das erste Element im vollständigen Namen eines Antragstellers. Obwohl hier normalerweise der Vorname des Antragstellers angegeben wird, kann der Wert auch den zweiten Vornamen oder dessen Initiale umfassen.

Ausführungsstatus

Der Status der Verarbeitung einer Anforderung. Dieser Status wird im Aktionsprotokoll angezeigt. Eine Beschreibung der verschiedenen Statuswerte finden Sie in „Status der Registrierungsanforderungen“ auf Seite 67.

Nachname

Der Nach- oder Familienname des Antragstellers.

Vorhergehende Anforderungs-ID

Eine verschlüsselte Zeichenfolge, die für die ID steht, die für eine vorherige Registrierungsanforderung generiert wurde, wenn das Zertifikat erneuert wurde.

Registrierungsdomäne

Die Registrierungsdomäne, die gesicherte Ressourcen für den Eigner eines Zertifikats bereitstellt.

Anforderungs-ID

Eine verschlüsselte Zeichenfolge, die für die ID steht, die für eine Registrierungsanforderung generiert wurde.

Anforderungsprofilname

Mit dieser Option wird die Verarbeitung der Registrierungsanforderung gesteuert. Dieses Profil enthält eine Schablone für das Zertifikat. Die Werte in diesem Profil überschreiben alle anderen Änderungen, die Sie möglicherweise vorgenommen haben. Der Abschnitt „Zertifikatstypen“ auf Seite 62 enthält eine Beschreibung der Merkmale der Zertifikate, die den einzelnen Anforderungsprofilen zugeordnet sind.

Anmerkung: Im RA Desktop werden dem Registrator möglicherweise zwei Anforderungsprofile angezeigt. Hierbei kann eines unter den Attributen für Anforderungen und das andere bei den Basisattributen aufgelistet werden. Dies bedeutet, dass das Anforderungsprofil zu einem bestimmten Zeitpunkt von einem Registrator überschrieben wurde. Das Profil in den Attributen für die Anforderung wurde zusammen mit anderen Attributen der Registrierungsanforderung temporär inaktiviert. Das Profil in den Basisattributen ist das aktuelle Anforderungsprofil.

Anforderungsstatus

Der Status der Registrierungsanforderung. Dieser Status wird im Aktionsprotokoll angezeigt. Eine Beschreibung der verschiedenen Statuswerte finden Sie in „Status der Registrierungsanforderungen“ auf Seite 67.

Anforderungsvariablen

Werte, die der Antragsteller während des Registrierungsprozesses angegeben hat.

RA-Aktionen

Die folgenden Aktionen stehen für die Registrierungsfunktion und den Registrator zur Verfügung, um Registrierungsanforderungen zu verarbeiten:

Genehmigen

Mit dieser Option wird die Registrierungsanforderung genehmigt, damit dem Antragsteller das angeforderte Zertifikat ausgestellt werden kann.

Als 'anstehend' behalten

Mit dieser Option wird die Entscheidung verzögert. Verwenden Sie diese Option, wenn der Registrator zur Bearbeitung des Antrags noch externe Informationen benötigt oder lediglich einen Kommentar an den Datensatz anfügen will.

Zurückweisen

Mit dieser Option wird die Registrierungsanforderung zurückgewiesen.

Widerrufen

Mit dieser Option wird die Gültigkeit eines Zertifikates beendet.

Anmerkung: Wenn Sie ein Zertifikat widerrufen und als Begründung **Zertifikat in den Wartestatus setzen** angeben, können Sie diese Aktion später umkehren, es sei denn, der Gültigkeitszeitraum des Zertifikats ist in der Zwischenzeit abgelaufen. Um die Aktion umzukehren, müssen Sie den Widerruf einfach wiederholen und als Grund **Aus der CRL entfernen** angeben.

Anforderung als 'nicht erneuerbar' definieren

Mit dieser Option wird der Status eines erneuerbaren Zertifikats in 'nicht erneuerbar' geändert.

Anforderung als 'erneuerbar' definieren

Mit dieser Option wird der Status eines nicht erneuerbaren Zertifikats in 'erneuerbar' geändert.

Keine Aktion verfügbar

Diese Option gibt an, dass der Registrator lediglich über die Berechtigung zum Anzeigen der Datensätze in der Registrierungsdomäne verfügt.

Status der Registrierungsanforderungen

Alle Statuswerte stellen Ereignisse im Aktionsprotokoll der Anforderung oder des Zertifikats dar.

Anforderungsstatus

Genehmigt

Die Registrierungsanforderung wurde genehmigt.

Abgeschlossen

Ein RA-Prozess oder Registrator hat die Registrierungsanforderung entweder genehmigt oder zurückgewiesen. Bei einer genehmigten Anforderung wurde ein Zertifikat an den Benutzer gesendet.

Anmerkung: Dies ist der endgültige Anforderungsstatus für eine Registrierungsanforderung. Der Ausführungsstatus einer abgeschlossenen Anforderung verweist auf nachfolgende Aktionen und Ereignisse, die sich auf die Anforderung auswirken. Beispiel: Wird ein Zertifikat erneuert oder widerrufen, wird dies im Ausführungsstatus angegeben. Der Anforderungsstatus bleibt jedoch weiterhin 'Abgeschlossen'.

Anstehend

Die Registrierungsanforderung wurde möglicherweise bereits geprüft, die Entscheidung über Genehmigung oder Zurückweisung steht jedoch noch aus.

Empfangen

Eine Registrierungsanforderung wurde empfangen.

Nicht genehmigt

Die Registrierungsanforderung wurde zurückweisen. Es wurde kein Zertifikat ausgestellt.

Ausführungsstatus

Übergeben

Das Zertifikat wurde an die Webseite übergeben, auf der es vom Benutzer akzeptiert werden kann.

Übergabe bestätigt

Der Benutzer hat das Zertifikat auf den Webbrowser heruntergeladen.

Ausgestellt

Die Registrierungsanforderung wurde genehmigt und das Zertifikat ausgestellt.

Nicht ausgestellt

Das Zertifikat wurde noch nicht ausgestellt. Dieser Status gibt nicht an, ob für die Anforderung bereits eine Aktion ausgeführt wurde.

Erneuert

Das einem bestimmten Datensatz zugeordnete Zertifikat wurde erneuert. Hierdurch werden ein neuer Datensatz und ein neues Zertifikat generiert.

Widerrufen

Das einem bestimmten Datensatz zugeordnete Zertifikat wurde widerrufen und als ungültig definiert.

6

Anpassungsbeispiel

Um die Anforderungen Ihres Unternehmens optimal zu erfüllen, können Sie mit Tivoli PKI zahlreiche Komponenten Ihrer Registrierungsdomäne anpassen.

Dieses Kapitel zeigt, wie verschiedene Elemente in Tivoli PKI angepasst werden können. Es erläutert anhand eines Anpassungsbeispiels das Planen, Identifizieren, Implementieren und Prüfen von Elementen, die in Tivoli PKI angepasst werden können.

Sie können den Tivoli PKI-Server so anpassen, dass er folgende Bedingungen erfüllt und zur Ausführung der u. a. Operationen verwendet werden kann:

- Einsetzbarkeit in verschiedenen Ländern, Unternehmen bzw. Abteilungen.
- Erfassen von für das Unternehmen relevanten Daten bei der Registrierung und Zertifizierung.
- Ändern der Darstellung von Web-Seiten.
- Integrieren abweichender Terminologie für die Hilfefunktion auf Web-Seiten.
- Erstellen angepasster Zertifikatstypen.
- Prüfen der auf der Registrierungsseite angegebenen Informationen.
- Anwenden von Unternehmensregeln auf die Registrierung, Zertifizierung und Verwaltung.
- Zurückkehren zur angepassten Unternehmenswebsite nach dem Herunterladen des Zertifikats.
- Einbinden des IBM Directory-Servers in Ihre Unternehmenshierarchie.

Planen der Anpassung

Neben dem Analysieren, Bewerten und Planen der für die Implementierung relevanten Faktoren sind die Darstellung der Verzeichnisstruktur und das Auflisten aller Anforderungen eines Unternehmens die wichtigsten Arbeitsschritte bei der individuellen Anpassung von Tivoli PKI. Das erweiterte Beispiel in diesem Kapitel beschreibt, wie das Beispielunternehmen "LoTo Organization" seinen Tivoli PKI-Server anpasst.

Verzeichnisstruktur des Unternehmens

LoTo Organization ist in drei verschiedenen Ländern tätig und führt seine Geschäfte unter vier, regional unterschiedlichen Namen. Jedes der vier Regionalunternehmen ist in vier Abteilungen untergliedert.

■ LoTo Organization:

- Länder:
 - USA
 - Spanien
 - Großbritannien
- Regionalunternehmen:
 - Business United Garages Enterprises (BUGS)
 - Delta Auto Factory (DAF)
 - Printing of Kits LTD (POK)
 - Treats World Incorp (TWI)

Identifizieren der kundenspezifischen Anforderungen

Im Folgenden finden Sie eine Liste mit Beispielanforderungen und -implementierungen für LoTo Organization:

Anpassbares Element	Anforderungen
Zertifikatstypen	Universelle Zertifikate mit einer Gültigkeitsdauer von einem Jahr oder zwei Jahren, die den Web-Client, die E-Mail-Funktion und das digitale Unterzeichnen unterstützen und Browserzertifikatsoptionen auf der Browserregistrierungsseite ersetzen.
Web-Seiten	LoTo Organization benötigt keine Änderungen an den Server-Seiten für die Zertifikatsregistrierung und die Vorabregistrierung. Ändern der Titel und Hilfeelemente auf den Registrierungsseiten und Entfernen der Vorabregistrierung aus der Liste der möglichen Auswahloptionen.
Grafiken	Ersetzen der Grafiken.
E-Mail-Benachrichtigungsbrief	Angaben des Firmennamens auf der E-Mail.
Erfassen von Kunden- und Mitarbeiterdaten	Entfernen der Elemente für die Angabe des Bundeslandes, Ortes und der Straße und Aufnehmen der Elemente für die Angabe des Unternehmens, der Abteilung und des Landes in das Auswahlmenü der verdeckten Liste.
Erfassen unternehmensrelevanter Kunden- und Mitarbeiterdaten	Erfassen der laufenden Mitarbeiternummer, des Jobtitels und der Versicherungsnummer.
Prüfen persönlicher Informationen	Prüfen, ob die laufende Mitarbeiternummer, der Jobtitel und die Versicherungsnummer auf der Registrierungsseite eingegeben wurden.
Ausführen von Regeln	Alle Member von /O=BUGS/OU=ITS /O=TWT/OU=DEV, für die eine automatische Genehmigung angefordert wurde.
Seite, zu der nach dem Herunterladen des Zertifikats zurückgekehrt wird	Zurückkehren auf die Homepage des Unternehmens, nachdem das Zertifikat heruntergeladen wurde.
Directory-Server	Anpassen des Directory-Servers zur Orientierung an der Unternehmenshierarchie.

Identifizieren der zu ändernden Dateien

Die folgende Tabelle enthält die Dateien, an denen bei der Anpassung möglicherweise Änderungen vorgenommen werden müssen:

Anpassbares Element	Zweck	Dateiname
Index/Homepage	Homepage	index.jsp
Registrierungsformulare für alle Registrierungstypen	Browser Netscape Browser Internet Explorer Server- oder Einheitenvorabregistrierung	NSBbrowserSSLCert_Enroll.jsp IEBrowserSSLCert_Enroll.jsp PKCS107Cert_Enroll.jsp PreReg_Enroll.jsp
Seiten für Benutzer-rückmeldungen	Fehlernachrichten Instruktionen nach dem Übergeben	TA_ErrorMsg.jsp *_CkStatus.jsp
Statusinformationen	Genehmigung Wartestatus Zurückweisung	*_Approved.jsp *_Pending.jsp *_Rejected.jsp
Erneuerungsformular für Browser-Zertifikate	Netscape Internet Explorer	NSBrowserSSLCert_Renew.jsp IEBrowserSSLCert_Renew.jsp
Zurückweisungsformular für Browser-Zertifikate	Netscape Internet Explorer	NSBrowserSSLCert_Revoke.jsp IEBrowserSSLCert_Revoke.jsp
Bildmaterial und Banner auf einer Registrierungsseite	Grafiken auf Web-Seiten Grafikdateien	NSBrowserSSLCert_RevokeRecd.jsp IEBrowserSSLCert_RevokeRecd.jsp
E-Mail-Benachrichtigungsbrief	E-Mail-Benachrichtigung zur Information über Genehmigung oder Zurückweisung einer Anforderung	*.ltr
Konfigurationsdatei der Registrierungs-funktion	Definiert die Komponenten und Werte in der Betriebsauswahlliste	raconfig.cfg
Regel-Exit	Unterstützt die automatische Genehmigung	auto_approve.exe<installationspfad>/pkrf/ samples/auto_approve.cpp für AIX <installationspfad>\pkrf\samples\ auto_approve.cpp für Windows NT
Zertifikatstypen	Speichert Informationen für unterstützte Zertifikate	certificate_profiles.cfg

RA Desktop	Web-Adresse, die dem Administrator nach Verlassen von RA Desktop angezeigt wird	radesktop.jsp
Konfigurationsdatei von RA Desktop	Konfigurationsdatei von RA Desktop	raprofiles.cfg
Directory-Server	Speichert Informationen zu gültigen und widerrufenen Zertifikaten	Siehe den folgenden Abschnitt

Die Dateien sind in einem der folgenden Verzeichnisse gespeichert:

Unter AIX:

```
/usr/lpp/iau/pkrf/Domains/<your domain>/webpages
/usr/lpp/iau/pkrf/Domains/<your domain>/etc
/usr/lpp/iau/pkrf/Domains/<your domain>/bin
```

Unter Windows NT:

```
<install path>\webpages
<install path>\etc
<install path>\bin
```

Hierbei steht *<your domain>* für die Registrierungsdomäne und *<install path>* für die vollständig qualifizierte Pfadangabe.

Änderungen vornehmen

Bei der Durchführung von Änderungen an den Dateien, die für die Registrierungsdomäne angepasst werden sollen, müssen Sie äußerst vorsichtig vorgehen. Vor dem Ändern einer Datei muss unbedingt eine Sicherungskopie erstellt werden. Die Verfügbarkeit einer Sicherungskopie ist besonders wichtig bei JSP-Dateien, der Konfigurationsdatei 'raconfig.cfg' sowie bei den Zertifikatsprofildateien.

1. Vor der Durchführung von Änderungen an einer Datei sollten Sie immer eine Sicherungskopie erstellen.
2. Wenn Tivoli PKI auf einer Maschine unter Windows NT installiert ist, müssen Sie die Dateinamen aller neuen Ressourcendateien (z. B. aller HTML- und JSP-Dateien), die für die Registrierungsanwendung erstellt werden, in Kleinbuchstaben angeben. Andernfalls gibt der IBM HTTP-Server für alle Dateinamen, die nur Großbuchstaben oder Buchstaben in Groß-/Kleinschreibung enthalten, möglicherweise die folgende Fehlermeldung zurück: " ERROR 404 NOT FOUND ". Beispiel: Ein gültiger Dateiname ist 'my.html'; ungültige Dateinamen sind 'MY.html' oder 'My.html'.
3. Verwenden Sie für Länder, für die in Tivoli PKI-Anwendungsdateien Nicht-ASCII-Zeichenwerte erforderlich sind, das UTF-8-codierte Unicode-Format. UTF-8-codierter Unicode erlaubt das universelle Codieren von Zeichen und ermöglicht Tivoli PKI die gleichzeitige Unterstützung mehrerer Sprachen auf dem selben System und sogar innerhalb eines Zertifikatsprofils. Wenn eine Datei UTF-8-codierte Daten enthält, sollten Sie beim Editieren mit besonderer Vorsicht vorgehen, um eine Beschädigung der UTF-8-Werte zu verhindern. Verwenden Sie aus diesem Grund einen Editor, der das Importieren

und Exportieren von UTF-8-Daten unterstützt. Hierzu gehören z. B. der Editor UniEdit unter Windows NT und das Tool 'iconv' unter AIX.

Im Folgenden sind Beispieländerungen aufgeführt, die an Tivoli PKI vorgenommen werden können:

Webseiten: Seitentitel und -beschreibungen ändern

Im LoTo Organization-Beispiel wollen Sie die Titel und die Beschriftung des Knopfes von "Identitätsnachweis - Verwaltung" in "Zertifikatsaussteller" und die Seitenbeschreibung in "LoTo Organization - Zertifikatsaussteller" ändern. Darüber hinaus soll die Option für die "Vorabregistrierung" von der Registrierungsseite entfernt werden.

Zunächst müssen Sie in allen JSP-Dateien (*.jsp) die Titel und die Beschriftung des Knopfes von "Identitätsnachweis - Verwaltung" in "Zertifikatsaussteller" und anschließend die Seitenbeschreibung in "LoTo Organization - Zertifikatsaussteller" ändern.

1. Ändern Sie in der Datei 'index.jsp' das folgende Element:

```
<% // Page Title %>
<tr>
<td HEIGHT="35" ALIGN="RIGHT" VALIGN="TOP">
<font SIZE="3" COLOR="#006699">
Identitätsnachweis - Verwaltung
</font>
</td>
</tr>
```

In folgendes Element:

```
<% // Page Title %>
<TR>
<TD HEIGHT="35" ALIGN="RIGHT" VALIGN="TOP">
<FONT SIZE="3" COLOR="#006699">
Zertifikatsaussteller
</FONT>
</TD>
</TR>
```

2. Ändern Sie das folgende Element:

```
<% // Page Description %>
<TITLE>Tivoli PKI Credential Enrollment</TITLE>
<META NAME="Description" CONTENT="Tivoli Public Key Infrastructure Credential
Enrollment">
```

In folgendes Element:

```
<% // Page Description %>
<TITLE> LoTo Organization Zertifikatsaussteller</TITLE>
<META NAME="Description" CONTENT="LoTo Organization Zertifikatsaussteller">
```

Die Auswahloption für die Vorabregistrierung kann nur von der Registrierungsseite entfernt werden. Die Registrierungsseite für die Vorabregistrierung kann unter 'http://<your server>/<your domain>/PreReg_Enroll.jsp/PreReg_Enroll.jsp' aufgerufen werden.

Wenn Sie die Option für die Vorabregistrierung aus der Registrierungsseite entfernen wollen, müssen Sie die Zeile für die Vorabregistrierung von Zertifikaten löschen:

1. Ändern Sie in der Datei 'index.jsp' das folgende Element:

```
<OPTION VALUE="30">Server or Device Certificate
<OPTION VALUE="40">Certificate Preregistration
</SELECT>
```

In folgendes Element:

```
<OPTION VALUE="30">Server or Device Certificate
</SELECT>
```

Sammeln von Kunden- und Mitarbeiterdaten

Im LoTo Organization-Beispiel wollen Sie die folgenden Änderungen an den Registrierungs-Web-Seiten im Browser vornehmen:

1. Elemente zur Angabe des Bundeslandes, Ortes und der Straße entfernen.
2. Elemente für die Angabe des Unternehmens, der Abteilung und des Landes in das Auswahlmenü der verdeckten Liste aufnehmen.

Gehen Sie wie folgt vor, um die Elemente zur Angabe des Bundeslandes, des Ortes und der Straße zu entfernen:

1. **Entfernen Sie die folgenden Codeblöcke aus der Datei 'NSBrowserSSLCert_Enroll.jsp':**

```
<% // Street Address (STREET) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[9] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[9] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[9] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="
<%= inputFieldNames[9] %>" SIZE="<%= sizeOfInputFields %>" MAXLENGTH="180"
VALUE="<%= inputFieldReturnValues[9] %>">
</TD>
</TR>
<% // Locality (L) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[10] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[10] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[10] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="
<%= inputFieldNames[10] %>" SIZE="<%= sizeOfInputFields %>" MAXLENGTH="128"
VALUE="<%= inputFieldReturnValues[10] %>">
</TD>
</TR>
```

```

<% // State (ST) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[11] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[11] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[11] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[11] %>" SIZE="<%=
sizeofInputFields %>" MAXLENGTH="128"
VALUE="<%= inputFieldReturnValues[11] %>">
</TD>
</TR>

```

2. **Entfernen Sie die folgenden Codeblöcke aus der Datei 'IEBrowserSSLCert_Enroll.jsp':**

```

DN += ",<%= inputFieldNames[8] %>=" +
document.CertReqForm.
<%= inputFieldNames[8] %>.value;
DN += ",<%= inputFieldNames[9] %>=" +
document.CertReqForm.
<%= inputFieldNames[9] %>.value;
DN += ",<%= inputFieldNames[10] %>=" +
document.CertReqForm.
<%= inputFieldNames[10] %>.value;

```

3. **Entfernen Sie die folgenden Codeblöcke aus der Datei 'IEBrowserSSLCert_Enroll.jsp':**

```

document.RegForm.
<%= inputFieldNames[9] %>.value
= document.CertReqForm.
<%= inputFieldNames[9] %>.value;
document.RegForm.
<%= inputFieldNames[10] %>.value =
document.CertReqForm.
<%= inputFieldNames[10] %>.value;
document.RegForm.
<%= inputFieldNames[11] %>.value =
document.CertReqForm.
<%= inputFieldNames[11] %>.value;

```

4. **Entfernen Sie die folgenden Codeblöcke aus der Datei 'IEBrowserSSLCert_Enroll.jsp':**

```

<% // Street Address (STREET) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[9] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[9] %>
<%= STRING_Colon %>

```

```

</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[9] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="
<%= inputFieldNames[9] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="180"
VALUE="<%= inputFieldReturnValues[9] %>">
</TD>
</TR>

<% // Locality (L) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[10] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[10] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[10] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="
<%= inputFieldNames[10] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="128"
VALUE="<%= inputFieldReturnValues[10] %>">
</TD>
</TR>

<% // State (ST) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[11] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[11] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[11] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="
<%= inputFieldNames[11] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="128"
VALUE="<%= inputFieldReturnValues[11] %>">
</TD>
</TR>

```

Gehen Sie wie folgt vor, um die Elemente für die Angabe des Unternehmens, der Abteilung und des Landes in das Auswahlménü der verdeckten Liste aufzunehmen:

1. Entfernen Sie den folgenden Codeblock aus der Datei 'NSBrowserSSLCert_Enroll.jsp':

```
<% // Organization (O) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[7] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[7] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[7] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[7] %>" SIZE="<%= sizeofInputFields
%>" MAXLENGTH="64" VALUE="<%= inputFieldReturnValues[7] %>">
</TD>
</TR>

<% // Organizational Unit (OU) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[8] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[8] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[8] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[8] %>" SIZE="<%= sizeofInputFields
%>" MAXLENGTH="64" VALUE="<%= inputFieldReturnValues[8] %>">
</TD>
</TR>
```

2. Entfernen Sie den folgenden Codeblock aus der Datei 'NSBrowserSSLCert_Enroll.jsp':

```
<% // Country (C) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[12] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
```

```

<%= STRING_InputFieldLbls[12] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[12] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[12] %>"
      SIZE="1">
<%
/*****
* Create dropdown list of ISO 3166 country names and codes:
* ftp://ftp.ripe.net/iso3166-countrycodes
*****/
* Optional Translatable Strings:
* STRING_CountryNames[0-238], leave the country
* name in English if not translatable.
*****/
*/
//-----
// Initialize arrays of country names and codes.
//-----
int numOfCountries = 239;
String[] STRING_CountryNames = new
String[numOfCountries];
String[] countryCodes = new
String[numOfCountries];

countryCodes[0] = "AF";
countryCodes[1] = "AL";
countryCodes[2] = "DZ";
countryCodes[3] = "AS";
countryCodes[4] = "AD";
countryCodes[5] = "AO";
countryCodes[6] = "AI";
countryCodes[7] = "AQ";
countryCodes[8] = "AG";
countryCodes[9] = "AR";
countryCodes[10] = "AM";
countryCodes[11] = "AW";
countryCodes[12] = "AU";
countryCodes[13] = "AT";
countryCodes[14] = "AZ";
countryCodes[15] = "BS";
countryCodes[16] = "BH";
countryCodes[17] = "BD";
countryCodes[18] = "BB";
countryCodes[19] = "BY";
countryCodes[20] = "BE";
countryCodes[21] = "BZ";
countryCodes[22] = "BJ";
countryCodes[23] = "BM";
countryCodes[24] = "BT";
countryCodes[25] = "BO";
countryCodes[26] = "BA";
countryCodes[27] = "BW";
countryCodes[28] = "BV";
countryCodes[29] = "BR";
countryCodes[30] = "IO";
countryCodes[31] = "BN";
countryCodes[32] = "BG";
countryCodes[33] = "BF";
countryCodes[34] = "BI";
countryCodes[35] = "KH";
countryCodes[36] = "CM";
countryCodes[37] = "CA";

```

```
countryCodes[38] = "CV";
countryCodes[39] = "KY";
countryCodes[40] = "CF";
countryCodes[41] = "TD";
countryCodes[42] = "CL";
countryCodes[43] = "CN";
countryCodes[44] = "CX";
countryCodes[45] = "CC";
countryCodes[46] = "CO";
countryCodes[47] = "KM";
countryCodes[48] = "CG";
countryCodes[49] = "CD";
countryCodes[50] = "CK";
countryCodes[51] = "CR";
countryCodes[52] = "CI";
countryCodes[53] = "HR";
countryCodes[54] = "CU";
countryCodes[55] = "CY";
countryCodes[56] = "CZ";
countryCodes[57] = "DK";
countryCodes[58] = "DJ";
countryCodes[59] = "DM";
countryCodes[60] = "DO";
countryCodes[61] = "TP";
countryCodes[62] = "EC";
countryCodes[63] = "EG";
countryCodes[64] = "SV";
countryCodes[65] = "GQ";
countryCodes[66] = "ER";
countryCodes[67] = "EE";
countryCodes[68] = "ET";
countryCodes[69] = "FK";
countryCodes[70] = "FO";
countryCodes[71] = "FJ";
countryCodes[72] = "FI";
countryCodes[73] = "FR";
countryCodes[74] = "FX";
countryCodes[75] = "GF";
countryCodes[76] = "PF";
countryCodes[77] = "TF";
countryCodes[78] = "GA";
countryCodes[79] = "GM";
countryCodes[80] = "GE";
countryCodes[81] = "DE";
countryCodes[82] = "GH";
countryCodes[83] = "GI";
countryCodes[84] = "GR";
countryCodes[85] = "GL";
countryCodes[86] = "GD";
countryCodes[87] = "GP";
countryCodes[88] = "GU";
countryCodes[89] = "GT";
countryCodes[90] = "GN";
countryCodes[91] = "GW";
countryCodes[92] = "GY";
countryCodes[93] = "HT";
countryCodes[94] = "HM";
countryCodes[95] = "VA";
countryCodes[96] = "HN";
countryCodes[97] = "HK";
countryCodes[98] = "HU";
countryCodes[99] = "IS";
countryCodes[100] = "IN";
countryCodes[101] = "ID";
countryCodes[102] = "IR";
countryCodes[103] = "IQ";
countryCodes[104] = "IE";
```

```
countryCodes[105] = "IL";
countryCodes[106] = "IT";
countryCodes[107] = "JM";
countryCodes[108] = "JP";
countryCodes[109] = "JO";
countryCodes[110] = "KZ";
countryCodes[111] = "KE";
countryCodes[112] = "KI";
countryCodes[113] = "KP";
countryCodes[114] = "KR";
countryCodes[115] = "KW";
countryCodes[116] = "KG";
countryCodes[117] = "LA";
countryCodes[118] = "LV";
countryCodes[119] = "LB";
countryCodes[120] = "LS";
countryCodes[121] = "LR";
countryCodes[122] = "LY";
countryCodes[123] = "LI";
countryCodes[124] = "LT";
countryCodes[125] = "LU";
countryCodes[126] = "MO";
countryCodes[127] = "MK";
countryCodes[128] = "MG";
countryCodes[129] = "MW";
countryCodes[130] = "MY";
countryCodes[131] = "MV";
countryCodes[132] = "ML";
countryCodes[133] = "MT";
countryCodes[134] = "MH";
countryCodes[135] = "MQ";
countryCodes[136] = "MR";
countryCodes[137] = "MU";
countryCodes[138] = "YT";
countryCodes[139] = "MX";
countryCodes[140] = "FM";
countryCodes[141] = "MD";
countryCodes[142] = "MC";
countryCodes[143] = "MN";
countryCodes[144] = "MS";
countryCodes[145] = "MA";
countryCodes[146] = "MZ";
countryCodes[147] = "MM";
countryCodes[148] = "NA";
countryCodes[149] = "NR";
countryCodes[150] = "NP";
countryCodes[151] = "NL";
countryCodes[152] = "AN";
countryCodes[153] = "NC";
countryCodes[154] = "NZ";
countryCodes[155] = "NI";
countryCodes[156] = "NE";
countryCodes[157] = "NG";
countryCodes[158] = "NU";
countryCodes[159] = "NF";
countryCodes[160] = "MP";
countryCodes[161] = "NO";
countryCodes[162] = "OM";
countryCodes[163] = "PK";
countryCodes[164] = "PW";
countryCodes[165] = "PA";
countryCodes[166] = "PG";
countryCodes[167] = "PY";
countryCodes[168] = "PE";
countryCodes[169] = "PH";
countryCodes[170] = "PN";
countryCodes[171] = "PL";
```

```
countryCodes[172] = "PT";
countryCodes[173] = "PR";
countryCodes[174] = "QA";
countryCodes[175] = "RE";
countryCodes[176] = "RO";
countryCodes[177] = "RU";
countryCodes[178] = "RW";
countryCodes[179] = "KN";
countryCodes[180] = "LC";
countryCodes[181] = "VC";
countryCodes[182] = "WS";
countryCodes[183] = "SM";
countryCodes[184] = "ST";
countryCodes[185] = "SA";
countryCodes[186] = "SN";
countryCodes[187] = "SC";
countryCodes[188] = "SL";
countryCodes[189] = "SG";
countryCodes[190] = "SK";
countryCodes[191] = "SI";
countryCodes[192] = "SB";
countryCodes[193] = "SO";
countryCodes[194] = "ZA";
countryCodes[195] = "GS";
countryCodes[196] = "ES";
countryCodes[197] = "LK";
countryCodes[198] = "SH";
countryCodes[199] = "PM";
countryCodes[200] = "SD";
countryCodes[201] = "SR";
countryCodes[202] = "SJ";
countryCodes[203] = "SZ";
countryCodes[204] = "SE";
countryCodes[205] = "CH";
countryCodes[206] = "SY";
countryCodes[207] = "TW";
countryCodes[208] = "TJ";
countryCodes[209] = "TZ";
countryCodes[210] = "TH";
countryCodes[211] = "TG";
countryCodes[212] = "TK";
countryCodes[213] = "TO";
countryCodes[214] = "TT";
countryCodes[215] = "TN";
countryCodes[216] = "TR";
countryCodes[217] = "TM";
countryCodes[218] = "TC";
countryCodes[219] = "TV";
countryCodes[220] = "UG";
countryCodes[221] = "UA";
countryCodes[222] = "AE";
countryCodes[223] = "GB";
countryCodes[224] = "US";
countryCodes[225] = "UM";
countryCodes[226] = "UY";
countryCodes[227] = "UZ";
countryCodes[228] = "VU";
countryCodes[229] = "VE";
countryCodes[230] = "VN";
countryCodes[231] = "VG";
countryCodes[232] = "VI";
countryCodes[233] = "WF";
countryCodes[234] = "EH";
countryCodes[235] = "YE";
countryCodes[236] = "YU";
countryCodes[237] = "ZM";
countryCodes[238] = "ZW";
```

```
STRING_CountryNames[0] = "Afghanistan";
STRING_CountryNames[1] = "Albania";
STRING_CountryNames[2] = "Algeria";
STRING_CountryNames[3] = "American Samoa";
STRING_CountryNames[4] = "Andorra";
STRING_CountryNames[5] = "Angola";
STRING_CountryNames[6] = "Anguilla";
STRING_CountryNames[7] = "Antarctica";
STRING_CountryNames[8] = "Antigua And Barbuda";
STRING_CountryNames[9] = "Argentina";
STRING_CountryNames[10] = "Armenia";
STRING_CountryNames[11] = "Aruba";
STRING_CountryNames[12] = "Australia";
STRING_CountryNames[13] = "Austria";
STRING_CountryNames[14] = "Azerbaijan";
STRING_CountryNames[15] = "Bahamas";
STRING_CountryNames[16] = "Bahrain";
STRING_CountryNames[17] = "Bangladesh";
STRING_CountryNames[18] = "Barbados";
STRING_CountryNames[19] = "Belarus";
STRING_CountryNames[20] = "Belgium";
STRING_CountryNames[21] = "Belizev";
STRING_CountryNames[22] = "Benin";
STRING_CountryNames[23] = "Bermuda";
STRING_CountryNames[24] = "Bhutan";
STRING_CountryNames[25] = "Bolivia";
STRING_CountryNames[26] = "Bosnia And Herzegowina";
STRING_CountryNames[27] = "Botswana";
STRING_CountryNames[28] = "Bouvet Island";
STRING_CountryNames[29] = "Brazil";
STRING_CountryNames[30] = "British Indian Ocean Territory";
STRING_CountryNames[31] = "Brunei Darussalam";
STRING_CountryNames[32] = "Bulgaria";
STRING_CountryNames[33] = "Burkina Faso";
STRING_CountryNames[34] = "Burundi";
STRING_CountryNames[35] = "Cambodia";
STRING_CountryNames[36] = "Cameroon";
STRING_CountryNames[37] = "Canada";
STRING_CountryNames[38] = "Cape Verde";
STRING_CountryNames[39] = "Cayman Islands";
STRING_CountryNames[40] = "Central African Republic";
STRING_CountryNames[41] = "Chad";
STRING_CountryNames[42] = "Chile";
STRING_CountryNames[43] = "China";
STRING_CountryNames[44] = "Christmas Island";
STRING_CountryNames[45] = "Cocos (Keeling) Islands";
STRING_CountryNames[46] = "Colombia";
STRING_CountryNames[47] = "Comoros";
STRING_CountryNames[48] = "Congo";
STRING_CountryNames[49] = "Congo, The Democratic Republic Of The";
STRING_CountryNames[50] = "Cook Islands";
STRING_CountryNames[51] = "Costa Rica";
STRING_CountryNames[52] = "Cote D'ivoire";
STRING_CountryNames[53] = "Croatia (Local Name: Hrvatska)";
STRING_CountryNames[54] = "Cuba";
STRING_CountryNames[55] = "Cyprus";
STRING_CountryNames[56] = "Czech Republic";
STRING_CountryNames[57] = "Denmark";
STRING_CountryNames[58] = "Djibouti";
STRING_CountryNames[59] = "Dominica";
STRING_CountryNames[60] = "Dominican Republic";
STRING_CountryNames[61] = "East Timor";
STRING_CountryNames[62] = "Ecuador";
STRING_CountryNames[63] = "Egypt";
STRING_CountryNames[64] = "El Salvador";
STRING_CountryNames[65] = "Equatorial Guinea";
```

```

STRING_CountryNames[66] = "Eritrea";
STRING_CountryNames[67] = "Estonia";
STRING_CountryNames[68] = "Ethiopia";
STRING_CountryNames[69] = "Falkland Islands (Malvinas)";
STRING_CountryNames[70] = "Faroe Islands";
STRING_CountryNames[71] = "Fiji";
STRING_CountryNames[72] = "Finland";
STRING_CountryNames[73] = "France";
STRING_CountryNames[74] = "France, Metropolitan";
STRING_CountryNames[75] = "French Guiana";
STRING_CountryNames[76] = "French Polynesia";
STRING_CountryNames[77] = "French Southern Territories";
STRING_CountryNames[78] = "Gabon";
STRING_CountryNames[79] = "Gambia";
STRING_CountryNames[80] = "Georgia";
STRING_CountryNames[81] = "Germany";
STRING_CountryNames[82] = "Ghana";
STRING_CountryNames[83] = "Gibraltar";
STRING_CountryNames[84] = "Greece";
STRING_CountryNames[85] = "Greenland";
STRING_CountryNames[86] = "Grenada";
STRING_CountryNames[87] = "Guadeloupe";
STRING_CountryNames[88] = "Guam";
STRING_CountryNames[89] = "Guatemala";
STRING_CountryNames[90] = "Guinea";
STRING_CountryNames[91] = "Guinea-Bissau";
STRING_CountryNames[92] = "Guyana";
STRING_CountryNames[93] = "Haiti";
STRING_CountryNames[94] = "Heard And Mc Donald Islands";
STRING_CountryNames[95] = "Holy See (Vatican City State)";
STRING_CountryNames[96] = "Honduras";
STRING_CountryNames[97] = "China (Hong Kong S.A.R.)";
STRING_CountryNames[98] = "Hungary";
STRING_CountryNames[99] = "Iceland";
STRING_CountryNames[100] = "India";
STRING_CountryNames[101] = "Indonesia";
STRING_CountryNames[102] = "Iran (Islamic Republic Of)";
STRING_CountryNames[103] = "Iraq";
STRING_CountryNames[104] = "Ireland";
STRING_CountryNames[105] = "Israel";
STRING_CountryNames[106] = "Italy";
STRING_CountryNames[107] = "Jamaica";
STRING_CountryNames[108] = "Japan";
STRING_CountryNames[109] = "Jordan";
STRING_CountryNames[110] = "Kazakhstan";
STRING_CountryNames[111] = "Kenya";
STRING_CountryNames[112] = "Kiribati";
STRING_CountryNames[113] = "Korea, Democratic People's Republic Of";
STRING_CountryNames[114] = "Korea, Republic Of";
STRING_CountryNames[115] = "Kuwait";
STRING_CountryNames[116] = "Kyrgyzstan";
STRING_CountryNames[117] = "Lao People's Democratic Republic";
STRING_CountryNames[118] = "Latvia";
STRING_CountryNames[119] = "Lebanon";
STRING_CountryNames[120] = "Lesotho";
STRING_CountryNames[121] = "Liberia";
STRING_CountryNames[122] = "Libyan Arab Jamahiriya";
STRING_CountryNames[123] = "Liechtenstein";
STRING_CountryNames[124] = "Lithuania";
STRING_CountryNames[125] = "Luxembourg";
STRING_CountryNames[126] = "China (Macau S.A.R.)";
STRING_CountryNames[127] = "Macedonia, The Former Yugoslav Republic Of";
STRING_CountryNames[128] = "Madagascar";
STRING_CountryNames[129] = "Malawi";
STRING_CountryNames[130] = "Malaysia";
STRING_CountryNames[131] = "Maldives";
STRING_CountryNames[132] = "Mali";

```

```

STRING_CountryNames[133] = "Malta";
STRING_CountryNames[134] = "Marshall Islands";
STRING_CountryNames[135] = "Martinique";
STRING_CountryNames[136] = "Mauritania";
STRING_CountryNames[137] = "Mauritius";
STRING_CountryNames[138] = "Mayotte";
STRING_CountryNames[139] = "Mexico";
STRING_CountryNames[140] = "Micronesia, Federated States Of";
STRING_CountryNames[141] = "Moldova, Republic Of";
STRING_CountryNames[142] = "Monaco";
STRING_CountryNames[143] = "Mongoliav";
STRING_CountryNames[144] = "Montserrat";
STRING_CountryNames[145] = "Morocco";
STRING_CountryNames[146] = "Mozambique";
STRING_CountryNames[147] = "Myanmar";
STRING_CountryNames[148] = "Namibia";
STRING_CountryNames[149] = "Nauru";
STRING_CountryNames[150] = "Nepal";
STRING_CountryNames[151] = "Netherlands";
STRING_CountryNames[152] = "Netherlands Antilles";
STRING_CountryNames[153] = "New Caledonia";
STRING_CountryNames[154] = "New Zealand";
STRING_CountryNames[155] = "Nicaragua";
STRING_CountryNames[156] = "Niger";
STRING_CountryNames[157] = "Nigeria";
STRING_CountryNames[158] = "Niue";
STRING_CountryNames[159] = "Norfolk Island";
STRING_CountryNames[160] = "Northern Mariana Islands";
STRING_CountryNames[161] = "Norway";
STRING_CountryNames[162] = "Oman";
STRING_CountryNames[163] = "Pakistan";
STRING_CountryNames[164] = "Palau";
STRING_CountryNames[165] = "Panama";
STRING_CountryNames[166] = "Papua New Guinea";
STRING_CountryNames[167] = "Paraguay";
STRING_CountryNames[168] = "Peru";
STRING_CountryNames[169] = "Philippines";
STRING_CountryNames[170] = "Pitcairn";
STRING_CountryNames[171] = "Poland";
STRING_CountryNames[172] = "Portugal";
STRING_CountryNames[173] = "Puerto Rico";
STRING_CountryNames[174] = "Qatar";
STRING_CountryNames[175] = "Reunion";
STRING_CountryNames[176] = "Romania";
STRING_CountryNames[177] = "Russian Federation";
STRING_CountryNames[178] = "Rwanda";
STRING_CountryNames[179] = "Saint Kitts And Nevis";
STRING_CountryNames[180] = "Saint Lucia";
STRING_CountryNames[181] = "Saint Vincent And The Grenadines";
STRING_CountryNames[182] = "Samoa";
STRING_CountryNames[183] = "San Marino";
STRING_CountryNames[184] = "Sao Tome And Principe";
STRING_CountryNames[185] = "Saudi Arabia";
STRING_CountryNames[186] = "Senegal";
STRING_CountryNames[187] = "Seychelles";
STRING_CountryNames[188] = "Sierra Leone";
STRING_CountryNames[189] = "Singapore";
STRING_CountryNames[190] = "Slovakia (Slovak Republic)";
STRING_CountryNames[191] = "Slovenia";
STRING_CountryNames[192] = "Solomon Islands";
STRING_CountryNames[193] = "Somalia";
STRING_CountryNames[194] = "South Africa";
STRING_CountryNames[195] = "South Georgia And The South Sandwich Islands";
STRING_CountryNames[196] = "Spain";
STRING_CountryNames[197] = "Sri Lanka";
STRING_CountryNames[198] = "St. Helena";
STRING_CountryNames[199] = "St. Pierre And Miquelon";

```

```

STRING_CountryNames[200] = "Sudan";
STRING_CountryNames[201] = "Suriname";
STRING_CountryNames[202] = "Svalbard And Jan Mayen Islands";
STRING_CountryNames[203] = "Swaziland";
STRING_CountryNames[204] = "Sweden";
STRING_CountryNames[205] = "Switzerland";
STRING_CountryNames[206] = "Syrian Arab Republic";
STRING_CountryNames[207] = "Taiwan";
STRING_CountryNames[208] = "Tajikistan";
STRING_CountryNames[209] = "Tanzania, United Republic Of";
STRING_CountryNames[210] = "Thailand";
STRING_CountryNames[211] = "Togo";
STRING_CountryNames[212] = "Tokelau";
STRING_CountryNames[213] = "Tonga";
STRING_CountryNames[214] = "Trinidad And Tobago";
STRING_CountryNames[215] = "Tunisia";
STRING_CountryNames[216] = "Turkey";
STRING_CountryNames[217] = "Turkmenistan";
STRING_CountryNames[218] = "Turks And Caicos Islands";
STRING_CountryNames[219] = "Tuvalu";
STRING_CountryNames[220] = "Uganda";
STRING_CountryNames[221] = "Ukraine";
STRING_CountryNames[222] = "United Arab Emirates";
STRING_CountryNames[223] = "United Kingdom";
STRING_CountryNames[224] = "United States";
STRING_CountryNames[225] = "United States Minor Outlying Islands";
STRING_CountryNames[226] = "Uruguay";
STRING_CountryNames[227] = "Uzbekistan";
STRING_CountryNames[228] = "Vanuatu";
STRING_CountryNames[229] = "Venezuela";
STRING_CountryNames[230] = "Viet Nam";
STRING_CountryNames[231] = "Virgin Islands (British)";
STRING_CountryNames[232] = "Virgin Islands (U.S.)";
STRING_CountryNames[233] = "Wallis And Futuna Islands";
STRING_CountryNames[234] = "Western Sahara";
STRING_CountryNames[235] = "Yemen";
STRING_CountryNames[236] = "Yugoslavia";
STRING_CountryNames[237] = "Zambia";
STRING_CountryNames[238] = "Zimbabwe";

//-----
// Determine the selected country.
//-----
String selectedCountryCode =
request.getParameter( inputFieldNames[12] );
if ( selectedCountryCode == null ||
selectedCountryCode.equals("") ) {
selectedCountryCode = (String)
request.getAttribute( inputFieldNames[12] );
}
if ( selectedCountryCode == null ||
selectedCountryCode.equals("") ) {
selectedCountryCode = defaultCountryCode;
}

//-----
// Generate the Country dropdown list items
//-----

for ( int i = 0; i
< numOfCountries; i++ ) {
// Determine if current item
needs to be preselected.
if ( countryCodes[i].equals
(selectedCountryCode) ) {
selectedLbl = " SELECTED";
}
}

```

```

else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"\" + countryCodes[i] + "\"" + selectedLbl + ">" +
STRING_CountryNames[i] + " (" + countryCodes[i] + ")");
}
%>
</SELECT>
</TD>
</TR>

```

3. Der Ersatzcode lautet folgendermaßen:

```

<% // Organization (0) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[7] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[7] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[7] %>
</FONT>
<BR>
<SELECT NAME="<%=
inputFieldNames[7] %>" SIZE="1">
<%
/*****
* Create dropdown list of 0:
*****/
//-----
// Initialize arrays of Organization
names and codes.
//-----
int numOfOrg = 4;
String[] STRING_0 = new String[numOfOrg];
String[] oCodes = new String[numOfOrg];

oCodes[0] = "BUGS";
oCodes[1] = "DAF";
oCodes[2] = "POK";
oCodes[3] = "TWT";

STRING_0[0] = "Business United Garages Enterprises";
STRING_0[1] = "Delta Auto Factory";
STRING_0[2] = "Printing of Kits LTD";
STRING_0[3] = "Treats World Incorp";

//-----
// Determine the selected o.
//-----
String selectedOC = request.getParameter
( inputFieldNames[7]);
if ( selectedOC == null ||
selectedOC.equals("") ) {
selectedOC = (String)

```

```

request.getAttribute( inputFieldNames[7] );
}
if ( selectedOC == null ||
selectedOC.equals("") ) {
selectedOC = "BUGS";
}

//-----
// Generate the O dropdown list items
//-----

for ( int i = 0; i < numOfOrg; i++ ) {
// Determine if current item needs to be preselected.
if ( oCodes[i].equals(selectedOC) ) {
selectedLb1 = " SELECTED";
}
else {
selectedLb1 = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + oCodes[i] + "\" + selectedLb1 + ">" + STRING_O[i] + "
(" + oCodes[i] + ")" );
}
%>
</SELECT>
</TD>

</TR>

<% // Organizational Unit (OU) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[8] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLb1s[8] %>
<%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLb1 %>
<%= errorFlags[8] %>
</FONT>
<BR>
<SELECT NAME="<%=
inputFieldNames[8] %>" SIZE="1">
<%
/*****
* Create dropdown list of OU:
*****/
*/
//-----
// Initialize arrays of OU names and codes.
//-----
int numOfOrgUnit = 5;
String[] STRING_OU =
new String[numOfOrgUnit];
String[] ouCodes =
new String[numOfOrgUnit];

ouCodes[0] = "ITS";
ouCodes[1] = "SVT";

```

```

ouCodes[2] = "MKT";
ouCodes[3] = "DEV";
ouCodes[4] = "OTH";

STRING_OU[0] = "Information Tech. Srvs.";
STRING_OU[1] = "System Test";
STRING_OU[2] = "Marketing";
STRING_OU[3] = "Development";
STRING_OU[4] = "Planning";

//-----
// Determine the selected ou.
//-----
String selectedOUC =
request.getParameter( inputFieldNames[8] );
if ( selectedOUC == null
|| selectedOUC.equals("") ) {
selectedOUC = (String)
request.getAttribute( inputFieldNames[8] );
}
if ( selectedOUC == null ||
selectedOUC.equals("") ) {
selectedOUC = "ITS";
}

//-----
// Generate the OU dropdown list items
//-----

for ( int i = 0; i < numOfOrgUnit; i++ ) {
// Determine if current item needs to be preselected.
if ( ouCodes[i].equals(selectedOUC) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + ouCodes[i] + "\" + selectedLbl + ">" + STRING_OU[i] + "
(" + ouCodes[i] + ")" );
}
%>
</SELECT>
</TD>

</TR>

<% // Country (C) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[12] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[12] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[12] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[12] %>" SIZE="1">

```

```

<%
/*****
* Create dropdown list of ISO 3166 country names and codes:
* ftp://ftp.ripe.net/iso3166-countrycodes
*****/
* Optional Translatable Strings:
* STRING_CountryNames[0-238], leave the country
* name in English if not translatable.
*****/
*/
//-----
// Initialize arrays of country names and codes.
//-----
int numOfCountries = 3;
String[] STRING_CountryNames = new String[numOfCountries];
String[] countryCodes = new String[numOfCountries];

countryCodes[0] = "ES";
countryCodes[1] = "GB";
countryCodes[2] = "US";

STRING_CountryNames[0] = "Spain";
STRING_CountryNames[1] = "United Kingdom";
STRING_CountryNames[2] = "United States";

//-----
// Determine the selected country.
//-----
String selectedCountryCode = request.getParameter( inputFieldNames[12] );
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = (String) request.getAttribute( inputFieldNames[12] );
}
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = defaultCountryCode;
}

//-----
// Generate the Country dropdown list items
//-----

for ( int i = 0; i < numOfCountries; i++ ) {
// Determine if current item needs to be preselected.
if ( countryCodes[i].equals(selectedCountryCode) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + countryCodes[i] + "\"" + selectedLbl + ">" +
STRING_CountryNames[i] +
" (" + countryCodes[i] + ")" );
}
}%>
</SELECT>
</TD>
</TR>

```

4. Entfernen Sie den folgenden Codeblock aus der Datei 'IEBrowserSSLCert_Enroll.jsp':

```

<% // Organization (0) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[7] %>
</FONT>

```

```

</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[7] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[7] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[7] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="64"
VALUE="<%= inputFieldReturnValues[7] %>">
</TD>
</TR>

<%= // Organizational Unit (OU) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[8] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[8] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[8] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[8] %>" SIZE="<%=
sizeOfInputFields %>" MAXLENGTH="64" VALUE="<%= inputFieldReturnValues[8] %>">
</TD>
</TR>

```

5. **Entfernen Sie den folgenden Codeblock aus der Datei 'IEBrowserSSLCert_Enroll.jsp':**

```

<%= // Country (C) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[12] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[12] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[12] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[12] %>" SIZE="1">
<%
/*****
* Create dropdown list of ISO 3166 country names and codes:
* ftp://ftp.ripe.net/iso3166-countrycodes

```

```

*****
* Optional Translatable Strings:
* STRING_CountryNames[0-238], leave the country
* name in English if not translatable.
*****
*/
//-----
// Initialize arrays of country names and codes.
//-----
int numOfCountries = 239;
String[] STRING_CountryNames = new String[numOfCountries];
String[] countryCodes = new String[numOfCountries];

countryCodes[0] = "AF";
countryCodes[1] = "AL";
countryCodes[2] = "DZ";
countryCodes[3] = "AS";
countryCodes[4] = "AD";
countryCodes[5] = "AO";
countryCodes[6] = "AI";
countryCodes[7] = "AQ";
countryCodes[8] = "AG";
countryCodes[9] = "AR";
countryCodes[10] = "AM";
countryCodes[11] = "AW";
countryCodes[12] = "AU";
countryCodes[13] = "AT";
countryCodes[14] = "AZ";
countryCodes[15] = "BS";
countryCodes[16] = "BH";
countryCodes[17] = "BD";
countryCodes[18] = "BB";
countryCodes[19] = "BY";
countryCodes[20] = "BE";
countryCodes[21] = "BZ";
countryCodes[22] = "BJ";
countryCodes[23] = "BM";
countryCodes[24] = "BT";
countryCodes[25] = "BO";
countryCodes[26] = "BA";
countryCodes[27] = "BW";
countryCodes[28] = "BV";
countryCodes[29] = "BR";
countryCodes[30] = "IO";
countryCodes[31] = "BN";
countryCodes[32] = "BG";
countryCodes[33] = "BF";
countryCodes[34] = "BI";
countryCodes[35] = "KH";
countryCodes[36] = "CM";
countryCodes[37] = "CA";
countryCodes[38] = "CV";
countryCodes[39] = "KY";
countryCodes[40] = "CF";
countryCodes[41] = "TD";
countryCodes[42] = "CL";
countryCodes[43] = "CN";
countryCodes[44] = "CX";
countryCodes[45] = "CC";
countryCodes[46] = "CO";
countryCodes[47] = "KM";
countryCodes[48] = "CG";
countryCodes[49] = "CD";
countryCodes[50] = "CK";
countryCodes[51] = "CR";
countryCodes[52] = "CI";
countryCodes[53] = "HR";

```

```
countryCodes[54] = "CU";
countryCodes[55] = "CY";
countryCodes[56] = "CZ";
countryCodes[57] = "DK";
countryCodes[58] = "DJ";
countryCodes[59] = "DM";
countryCodes[60] = "DO";
countryCodes[61] = "TP";
countryCodes[62] = "EC";
countryCodes[63] = "EG";
countryCodes[64] = "SV";
countryCodes[65] = "GQ";
countryCodes[66] = "ER";
countryCodes[67] = "EE";
countryCodes[68] = "ET";
countryCodes[69] = "FK";
countryCodes[70] = "FO";
countryCodes[71] = "FJ";
countryCodes[72] = "FI";
countryCodes[73] = "FR";
countryCodes[74] = "FX";
countryCodes[75] = "GF";
countryCodes[76] = "PF";
countryCodes[77] = "TF";
countryCodes[78] = "GA";
countryCodes[79] = "GM";
countryCodes[80] = "GE";
countryCodes[81] = "DE";
countryCodes[82] = "GH";
countryCodes[83] = "GI";
countryCodes[84] = "GR";
countryCodes[85] = "GL";
countryCodes[86] = "GD";
countryCodes[87] = "GP";
countryCodes[88] = "GU";
countryCodes[89] = "GT";
countryCodes[90] = "GN";
countryCodes[91] = "GW";
countryCodes[92] = "GY";
countryCodes[93] = "HT";
countryCodes[94] = "HM";
countryCodes[95] = "VA";
countryCodes[96] = "HN";
countryCodes[97] = "HK";
countryCodes[98] = "HU";
countryCodes[99] = "IS";
countryCodes[100] = "IN";
countryCodes[101] = "ID";
countryCodes[102] = "IR";
countryCodes[103] = "IQ";
countryCodes[104] = "IE";
countryCodes[105] = "IL";
countryCodes[106] = "IT";
countryCodes[107] = "JM";
countryCodes[108] = "JP";
countryCodes[109] = "JO";
countryCodes[110] = "KZ";
countryCodes[111] = "KE";
countryCodes[112] = "KI";
countryCodes[113] = "KP";
countryCodes[114] = "KR";
countryCodes[115] = "KW";
countryCodes[116] = "KG";
countryCodes[117] = "LA";
countryCodes[118] = "LV";
countryCodes[119] = "LB";
countryCodes[120] = "LS";
```

```
countryCodes[121] = "LR";
countryCodes[122] = "LY";
countryCodes[123] = "LI";
countryCodes[124] = "LT";
countryCodes[125] = "LU";
countryCodes[126] = "MO";
countryCodes[127] = "MK";
countryCodes[128] = "MG";
countryCodes[129] = "MW";
countryCodes[130] = "MY";
countryCodes[131] = "MV";
countryCodes[132] = "ML";
countryCodes[133] = "MT";
countryCodes[134] = "MH";
countryCodes[135] = "MQ";
countryCodes[136] = "MR";
countryCodes[137] = "MU";
countryCodes[138] = "YT";
countryCodes[139] = "MX";
countryCodes[140] = "FM";
countryCodes[141] = "MD";
countryCodes[142] = "MC";
countryCodes[143] = "MN";
countryCodes[144] = "MS";
countryCodes[145] = "MA";
countryCodes[146] = "MZ";
countryCodes[147] = "MM";
countryCodes[148] = "NA";
countryCodes[149] = "NR";
countryCodes[150] = "NP";
countryCodes[151] = "NL";
countryCodes[152] = "AN";
countryCodes[153] = "NC";
countryCodes[154] = "NZ";
countryCodes[155] = "NI";
countryCodes[156] = "NE";
countryCodes[157] = "NG";
countryCodes[158] = "NU";
countryCodes[159] = "NF";
countryCodes[160] = "MP";
countryCodes[161] = "NO";
countryCodes[162] = "OM";
countryCodes[163] = "PK";
countryCodes[164] = "PW";
countryCodes[165] = "PA";
countryCodes[166] = "PG";
countryCodes[167] = "PY";
countryCodes[168] = "PE";
countryCodes[169] = "PH";
countryCodes[170] = "PN";
countryCodes[171] = "PL";
countryCodes[172] = "PT";
countryCodes[173] = "PR";
countryCodes[174] = "QA";
countryCodes[175] = "RE";
countryCodes[176] = "RO";
countryCodes[177] = "RU";
countryCodes[178] = "RW";
countryCodes[179] = "KN";
countryCodes[180] = "LC";
countryCodes[181] = "VC";
countryCodes[182] = "WS";
countryCodes[183] = "SM";
countryCodes[184] = "ST";
countryCodes[185] = "SA";
countryCodes[186] = "SN";
countryCodes[187] = "SC";
```

```

countryCodes[188] = "SL";
countryCodes[189] = "SG";
countryCodes[190] = "SK";
countryCodes[191] = "SI";
countryCodes[192] = "SB";
countryCodes[193] = "SO";
countryCodes[194] = "ZA";
countryCodes[195] = "GS";
countryCodes[196] = "ES";
countryCodes[197] = "LK";
countryCodes[198] = "SH";
countryCodes[199] = "PM";
countryCodes[200] = "SD";
countryCodes[201] = "SR";
countryCodes[202] = "SJ";
countryCodes[203] = "SZ";
countryCodes[204] = "SE";
countryCodes[205] = "CH";
countryCodes[206] = "SY";
countryCodes[207] = "TW";
countryCodes[208] = "TJ";
countryCodes[209] = "TZ";
countryCodes[210] = "TH";
countryCodes[211] = "TG";
countryCodes[212] = "TK";
countryCodes[213] = "TO";
countryCodes[214] = "TT";
countryCodes[215] = "TN";
countryCodes[216] = "TR";
countryCodes[217] = "TM";
countryCodes[218] = "TC";
countryCodes[219] = "TV";
countryCodes[220] = "UG";
countryCodes[221] = "UA";
countryCodes[222] = "AE";
countryCodes[223] = "GB";
countryCodes[224] = "US";
countryCodes[225] = "UM";
countryCodes[226] = "UY";
countryCodes[227] = "UZ";
countryCodes[228] = "VU";
countryCodes[229] = "VE";
countryCodes[230] = "VN";
countryCodes[231] = "VG";
countryCodes[232] = "VI";
countryCodes[233] = "WF";
countryCodes[234] = "EH";
countryCodes[235] = "YE";
countryCodes[236] = "YU";
countryCodes[237] = "ZM";
countryCodes[238] = "ZW";

STRING_CountryNames[0] = "Afghanistan";
STRING_CountryNames[1] = "Albania";
STRING_CountryNames[2] = "Algeria";
STRING_CountryNames[3] = "American Samoa";
STRING_CountryNames[4] = "Andorra";
STRING_CountryNames[5] = "Angola";
STRING_CountryNames[6] = "Anguilla";
STRING_CountryNames[7] = "Antarctica";
STRING_CountryNames[8] = "Antigua And Barbuda";
STRING_CountryNames[9] = "Argentina";
STRING_CountryNames[10] = "Armenia";
STRING_CountryNames[11] = "Aruba";
STRING_CountryNames[12] = "Australia";
STRING_CountryNames[13] = "Austria";
STRING_CountryNames[14] = "Azerbaijan";

```

```

STRING_CountryNames[15] = "Bahamas";
STRING_CountryNames[16] = "Bahrain";
STRING_CountryNames[17] = "Bangladesh";
STRING_CountryNames[18] = "Barbados";
STRING_CountryNames[19] = "Belarus";
STRING_CountryNames[20] = "Belgium";
STRING_CountryNames[21] = "Belizev";
STRING_CountryNames[22] = "Benin";
STRING_CountryNames[23] = "Bermuda";
STRING_CountryNames[24] = "Bhutan";
STRING_CountryNames[25] = "Bolivia";
STRING_CountryNames[26] = "Bosnia And Herzegowina";
STRING_CountryNames[27] = "Botswana";
STRING_CountryNames[28] = "Bouvet Island";
STRING_CountryNames[29] = "Brazil";
STRING_CountryNames[30] = "British Indian Ocean Territory";
STRING_CountryNames[31] = "Brunei Darussalam";
STRING_CountryNames[32] = "Bulgaria";
STRING_CountryNames[33] = "Burkina Faso";
STRING_CountryNames[34] = "Burundi";
STRING_CountryNames[35] = "Cambodia";
STRING_CountryNames[36] = "Cameroon";
STRING_CountryNames[37] = "Canada";
STRING_CountryNames[38] = "Cape Verde";
STRING_CountryNames[39] = "Cayman Islands";
STRING_CountryNames[40] = "Central African Republic";
STRING_CountryNames[41] = "Chad";
STRING_CountryNames[42] = "Chile";
STRING_CountryNames[43] = "China";
STRING_CountryNames[44] = "Christmas Island";
STRING_CountryNames[45] = "Cocos (Keeling) Islands";
STRING_CountryNames[46] = "Colombia";
STRING_CountryNames[47] = "Comoros";
STRING_CountryNames[48] = "Congo";
STRING_CountryNames[49] = "Congo, The Democratic Republic Of The";
STRING_CountryNames[50] = "Cook Islands";
STRING_CountryNames[51] = "Costa Rica";
STRING_CountryNames[52] = "Cote D'ivoire";
STRING_CountryNames[53] = "Croatia (Local Name: Hrvatska)";
STRING_CountryNames[54] = "Cuba";
STRING_CountryNames[55] = "Cyprus";
STRING_CountryNames[56] = "Czech Republic";
STRING_CountryNames[57] = "Denmark";
STRING_CountryNames[58] = "Djibouti";
STRING_CountryNames[59] = "Dominica";
STRING_CountryNames[60] = "Dominican Republic";
STRING_CountryNames[61] = "East Timor";
STRING_CountryNames[62] = "Ecuador";
STRING_CountryNames[63] = "Egypt";
STRING_CountryNames[64] = "El Salvador";
STRING_CountryNames[65] = "Equatorial Guinea";
STRING_CountryNames[66] = "Eritrea";
STRING_CountryNames[67] = "Estonia";
STRING_CountryNames[68] = "Ethiopia";
STRING_CountryNames[69] = "Falkland Islands (Malvinas)";
STRING_CountryNames[70] = "Faroe Islands";
STRING_CountryNames[71] = "Fiji";
STRING_CountryNames[72] = "Finland";
STRING_CountryNames[73] = "France";
STRING_CountryNames[74] = "France, Metropolitan";
STRING_CountryNames[75] = "French Guiana";
STRING_CountryNames[76] = "French Polynesia";
STRING_CountryNames[77] = "French Southern Territories";
STRING_CountryNames[78] = "Gabon";
STRING_CountryNames[79] = "Gambia";
STRING_CountryNames[80] = "Georgia";
STRING_CountryNames[81] = "Germany";

```

```

STRING_CountryNames[82] = "Ghana";
STRING_CountryNames[83] = "Gibraltar";
STRING_CountryNames[84] = "Greece";
STRING_CountryNames[85] = "Greenland";
STRING_CountryNames[86] = "Grenada";
STRING_CountryNames[87] = "Guadeloupe";
STRING_CountryNames[88] = "Guam";
STRING_CountryNames[89] = "Guatemala";
STRING_CountryNames[90] = "Guinea";
STRING_CountryNames[91] = "Guinea-Bissau";
STRING_CountryNames[92] = "Guyana";
STRING_CountryNames[93] = "Haiti";
STRING_CountryNames[94] = "Heard And Mc Donald Islands";
STRING_CountryNames[95] = "Holy See (Vatican City State)";
STRING_CountryNames[96] = "Honduras";
STRING_CountryNames[97] = "China (Hong Kong S.A.R.)";
STRING_CountryNames[98] = "Hungary";
STRING_CountryNames[99] = "Iceland";
STRING_CountryNames[100] = "India";
STRING_CountryNames[101] = "Indonesia";
STRING_CountryNames[102] = "Iran (Islamic Republic Of)";
STRING_CountryNames[103] = "Iraq";
STRING_CountryNames[104] = "Ireland";
STRING_CountryNames[105] = "Israel";
STRING_CountryNames[106] = "Italy";
STRING_CountryNames[107] = "Jamaica";
STRING_CountryNames[108] = "Japan";
STRING_CountryNames[109] = "Jordan";
STRING_CountryNames[110] = "Kazakhstan";
STRING_CountryNames[111] = "Kenya";
STRING_CountryNames[112] = "Kiribati";
STRING_CountryNames[113] = "Korea, Democratic People's Republic Of";
STRING_CountryNames[114] = "Korea, Republic Of";
STRING_CountryNames[115] = "Kuwait";
STRING_CountryNames[116] = "Kyrgyzstan";
STRING_CountryNames[117] = "Lao People's Democratic Republic";
STRING_CountryNames[118] = "Latvia";
STRING_CountryNames[119] = "Lebanon";
STRING_CountryNames[120] = "Lesotho";
STRING_CountryNames[121] = "Liberia";
STRING_CountryNames[122] = "Libyan Arab Jamahiriya";
STRING_CountryNames[123] = "Liechtenstein";
STRING_CountryNames[124] = "Lithuania";
STRING_CountryNames[125] = "Luxembourg";
STRING_CountryNames[126] = "China (Macau S.A.R.)";
STRING_CountryNames[127] = "Macedonia, The Former Yugoslav Republic Of";
STRING_CountryNames[128] = "Madagascar";
STRING_CountryNames[129] = "Malawi";
STRING_CountryNames[130] = "Malaysia";
STRING_CountryNames[131] = "Maldives";
STRING_CountryNames[132] = "Mali";
STRING_CountryNames[133] = "Malta";
STRING_CountryNames[134] = "Marshall Islands";
STRING_CountryNames[135] = "Martinique";
STRING_CountryNames[136] = "Mauritania";
STRING_CountryNames[137] = "Mauritius";
STRING_CountryNames[138] = "Mayotte";
STRING_CountryNames[139] = "Mexico";
STRING_CountryNames[140] = "Micronesia, Federated States Of";
STRING_CountryNames[141] = "Moldova, Republic Of";
STRING_CountryNames[142] = "Monaco";
STRING_CountryNames[143] = "Mongolia";
STRING_CountryNames[144] = "Montserrat";
STRING_CountryNames[145] = "Morocco";
STRING_CountryNames[146] = "Mozambique";
STRING_CountryNames[147] = "Myanmar";
STRING_CountryNames[148] = "Namibia";

```

```

STRING_CountryNames[149] = "Nauru";
STRING_CountryNames[150] = "Nepal";
STRING_CountryNames[151] = "Netherlands";
STRING_CountryNames[152] = "Netherlands Antilles";
STRING_CountryNames[153] = "New Caledonia";
STRING_CountryNames[154] = "New Zealand";
STRING_CountryNames[155] = "Nicaragua";
STRING_CountryNames[156] = "Niger";
STRING_CountryNames[157] = "Nigeria";
STRING_CountryNames[158] = "Niue";
STRING_CountryNames[159] = "Norfolk Island";
STRING_CountryNames[160] = "Northern Mariana Islands";
STRING_CountryNames[161] = "Norway";
STRING_CountryNames[162] = "Oman";
STRING_CountryNames[163] = "Pakistan";
STRING_CountryNames[164] = "Palau";
STRING_CountryNames[165] = "Panama";
STRING_CountryNames[166] = "Papua New Guinea";
STRING_CountryNames[167] = "Paraguay";
STRING_CountryNames[168] = "Peru";
STRING_CountryNames[169] = "Philippines";
STRING_CountryNames[170] = "Pitcairn";
STRING_CountryNames[171] = "Poland";
STRING_CountryNames[172] = "Portugal";
STRING_CountryNames[173] = "Puerto Rico";
STRING_CountryNames[174] = "Qatar";
STRING_CountryNames[175] = "Reunion";
STRING_CountryNames[176] = "Romania";
STRING_CountryNames[177] = "Russian Federation";
STRING_CountryNames[178] = "Rwanda";
STRING_CountryNames[179] = "Saint Kitts And Nevis";
STRING_CountryNames[180] = "Saint Lucia";
STRING_CountryNames[181] = "Saint Vincent And The Grenadines";
STRING_CountryNames[182] = "Samoa";
STRING_CountryNames[183] = "San Marino";
STRING_CountryNames[184] = "Sao Tome And Principe";
STRING_CountryNames[185] = "Saudi Arabia";
STRING_CountryNames[186] = "Senegal";
STRING_CountryNames[187] = "Seychelles";
STRING_CountryNames[188] = "Sierra Leone";
STRING_CountryNames[189] = "Singapore";
STRING_CountryNames[190] = "Slovakia (Slovak Republic)";
STRING_CountryNames[191] = "Slovenia";
STRING_CountryNames[192] = "Solomon Islands";
STRING_CountryNames[193] = "Somalia";
STRING_CountryNames[194] = "South Africa";
STRING_CountryNames[195] = "South Georgia And The South Sandwich Islands";
STRING_CountryNames[196] = "Spain";
STRING_CountryNames[197] = "Sri Lanka";
STRING_CountryNames[198] = "St. Helena";
STRING_CountryNames[199] = "St. Pierre And Miquelon";
STRING_CountryNames[200] = "Sudan";
STRING_CountryNames[201] = "Suriname";
STRING_CountryNames[202] = "Svalbard And Jan Mayen Islands";
STRING_CountryNames[203] = "Swaziland";
STRING_CountryNames[204] = "Sweden";
STRING_CountryNames[205] = "Switzerland";
STRING_CountryNames[206] = "Syrian Arab Republic";
STRING_CountryNames[207] = "Taiwan";
STRING_CountryNames[208] = "Tajikistan";
STRING_CountryNames[209] = "Tanzania, United Republic Of";
STRING_CountryNames[210] = "Thailand";
STRING_CountryNames[211] = "Togo";
STRING_CountryNames[212] = "Tokelau";
STRING_CountryNames[213] = "Tonga";
STRING_CountryNames[214] = "Trinidad And Tobago";
STRING_CountryNames[215] = "Tunisia";

```

```

STRING_CountryNames[216] = "Turkey";
STRING_CountryNames[217] = "Turkmenistan";
STRING_CountryNames[218] = "Turks And Caicos Islands";
STRING_CountryNames[219] = "Tuvalu";
STRING_CountryNames[220] = "Uganda";
STRING_CountryNames[221] = "Ukraine";
STRING_CountryNames[222] = "United Arab Emirates";
STRING_CountryNames[223] = "United Kingdom";
STRING_CountryNames[224] = "United States";
STRING_CountryNames[225] = "United States Minor Outlying Islands";
STRING_CountryNames[226] = "Uruguay";
STRING_CountryNames[227] = "Uzbekistan";
STRING_CountryNames[228] = "Vanuatu";
STRING_CountryNames[229] = "Venezuela";
STRING_CountryNames[230] = "Viet Nam";
STRING_CountryNames[231] = "Virgin Islands (British)";
STRING_CountryNames[232] = "Virgin Islands (U.S.)";
STRING_CountryNames[233] = "Wallis And Futuna Islands";
STRING_CountryNames[234] = "Western Sahara";
STRING_CountryNames[235] = "Yemen";
STRING_CountryNames[236] = "Yugoslavia";
STRING_CountryNames[237] = "Zambia";
STRING_CountryNames[238] = "Zimbabwe";

//-----
// Determine the selected country.
//-----
String selectedCountryCode = request.getParameter( inputFieldNames[12] );
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = (String) request.getAttribute( inputFieldNames[12] );
}
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = defaultCountryCode;
}

//-----
// Generate the Country dropdown list items
//-----

for ( int i = 0; i < numOfCountries; i++ ) {
// Determine if current item needs to be preselected.
if ( countryCodes[i].equals(selectedCountryCode) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + countryCodes[i] + "\"" + selectedLbl + ">" +
STRING_CountryNames[i] + " (" + countryCodes[i] + ")" );
}
%>
</SELECT>
</TD>
</TR>

```

6. Der Ersatzcode lautet folgendermaßen:

```

<% // Organization (0) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[7] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">

```

```

<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[7] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[7] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[7] %>" SIZE="1">
<%
/*****
* Create dropdown list of 0:
*****/
*/
//-----
// Initialize arrays of Organization names and codes.
//-----
int numOfOrg = 4;
String[] STRING_0 = new String[numOfOrg];
String[] oCodes = new String[numOfOrg];

oCodes[0] = "BUGS";
oCodes[1] = "DAF";
oCodes[2] = "POK";
oCodes[3] = "TWT";

STRING_0[0] = "Business United Garages Enterprises";
STRING_0[1] = "Delta Auto Factory";
STRING_0[2] = "Printing of Kits LTD";
STRING_0[3] = "Treats World Incorp";

//-----
// Determine the selected o.
//-----
String selectedOC = request.getParameter( inputFieldNames[7]);
if ( selectedOC == null || selectedOC.equals("") ) {
selectedOC = (String) request.getAttribute( inputFieldNames[7] );
}
if ( selectedOC == null || selectedOC.equals("") ) {
selectedOC = "BUGS";
}

//-----
// Generate the 0 dropdown list items
//-----

for ( int i = 0; i < numOfOrg; i++ ) {
// Determine if current item needs to be preselected.
if ( oCodes[i].equals(selectedOC) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + oCodes[i] + "\"" + selectedLbl + ">" +
STRING_0[i] +
" (" + oCodes[i] + ")" );
}
%>
</SELECT>
</TD>
</TR>

```

```

<% // Organizational Unit (OU) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[8] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[8] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[8] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[8] %>" SIZE="1">
<%
/*****
* Create dropdown list of OU:
*****/
//-----
// Initialize arrays of OU names and codes.
//-----
int numOfOrgUnit = 5;
String[] STRING_OU = new String[numOfOrgUnit];
String[] ouCodes = new String[numOfOrgUnit];

ouCodes[0] = "ITS";
ouCodes[1] = "SVT";
ouCodes[2] = "MKT";
ouCodes[3] = "DEV";
ouCodes[4] = "OTH";

STRING_OU[0] = "Information Tech. Srvs.";
STRING_OU[1] = "System Test";
STRING_OU[2] = "Marketing";
STRING_OU[3] = "Development";
STRING_OU[4] = "Planning";

//-----
// Determine the selected ou.
//-----
String selectedOUC = request.getParameter( inputFieldNames[8] );
if ( selectedOUC == null || selectedOUC.equals("") ) {
selectedOUC = (String) request.getAttribute( inputFieldNames[8] );
}
if ( selectedOUC == null || selectedOUC.equals("") ) {
selectedOUC = "ITS";
}

//-----
// Generate the OU dropdown list items
//-----

for ( int i = 0; i < numOfOrgUnit; i++ ) {
// Determine if current item needs to be preselected.
if ( ouCodes[i].equals(selectedOUC) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}
}

```

```

// Create the list item.
out.println( "<OPTION VALUE=\"\" + ouCodes[i] + "\"" + selectedLbl + ">" +
STRING_OU[i] +
" (" + ouCodes[i] + ")");
}
%>
</SELECT>
</TD>
</TR>

<% // Country (C) %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#FFE1C4">
<FONT SIZE="2">
<%= STRING_IntegerFieldHelps[12] %>
</FONT>
</TD>

<TD ALIGN="LEFT" BGCOLOR="#FFD1A4">
<FONT SIZE="2">
<STRONG>
<%= STRING_IntegerFieldLbls[12] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[12] %>
</FONT>
<BR>
<SELECT NAME="<%= inputFieldNames[12] %>" SIZE="1">
<%
/*****
* Create dropdown list of ISO 3166 country names and codes:
* ftp://ftp.ripe.net/iso3166-countrycodes
*****/
* Optional Translatable Strings:
* STRING_CountryNames[0-238], leave the country
* name in English if not translatable.
*****/
*/
//-----
// Initialize arrays of country names and codes.
//-----
int numOfCountries = 3;
String[] STRING_CountryNames = new String[numOfCountries];
String[] countryCodes = new String[numOfCountries];

countryCodes[0] = "ES";
countryCodes[1] = "GB";
countryCodes[2] = "US";

STRING_CountryNames[0] = "Spain";
STRING_CountryNames[1] = "United Kingdom";
STRING_CountryNames[2] = "United States";

//-----
// Determine the selected country.
//-----
String selectedCountryCode = request.getParameter( inputFieldNames[12] );
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = (String) request.getAttribute( inputFieldNames[12] );
}
if ( selectedCountryCode == null || selectedCountryCode.equals("") ) {
selectedCountryCode = defaultCountryCode;
}

//-----

```

```
// Generate the Country dropdown list items
//-----

for ( int i = 0; i < numOfCountries; i++ ) {
// Determine if current item needs to be preselected.
if ( countryCodes[i].equals(selectedCountryCode) ) {
selectedLbl = " SELECTED";
}
else {
selectedLbl = "";
}

// Create the list item.
out.println( "<OPTION VALUE=\"" + countryCodes[i] + "\" + selectedLbl + ">" +
STRING_CountryNames[i] +
" (" + countryCodes[i] + ")" );
}
%>
</SELECT>
</TD>
</TR>
```

Sammeln von unternehmensbezogenen Kunden- und Mitarbeiterdaten

Im LoTo Organization-Beispiel wollen Sie Mitarbeiterdaten aus der Browser-Registrierungsseite erfassen.

Auf den Browser-Registrierungs-Web-Seiten müssen Sie die Felder für die laufende Mitarbeiternummer, den Jobtitel und die Versicherungsnummer hinzufügen, um Daten zu erfassen.

Gehen Sie wie folgt vor, um die Felder für die laufende Mitarbeiternummer, den Jobtitel und die Versicherungsnummer hinzuzufügen:

1. Ändern Sie in der Datei 'NSBrowserSSLCert_Enroll.jsp' folgende Zeile:

```
int numOfInputFields = 14;
```

In folgende Zeile:

```
int numOfInputFields = 17;
```

2. Fügen Sie unter dem u. a. Codesegment:

```
inputFieldNames[13] = "domain_name";
STRING_InputFieldLbls[13] = "Domain Name";
STRING_InputFieldHelps[13] = "Type the domain name if you were instructed to do so.
For example, mypc.mydiv.mycorp.com.";
```

Folgenden Code hinzu:

```
inputFieldNames[14] = "SERIAL";
STRING_InputFieldLbls[14] = "Serial Number";
STRING_InputFieldHelps[14] = "Employee serial Number";
```

```
inputFieldNames[15] = "TITTLE";
STRING_InputFieldLbls[15] = "Job Tittle";
STRING_InputFieldHelps[15] = "Job Description Tittle";
```

```
inputFieldNames[16] = "SSN";
STRING_InputFieldLbls[16] = "Social Security Number";
STRING_InputFieldHelps[16] = "Socail Security Number";
```

3. Fügen Sie unter dem u. a. Codesegment:

```
<%
/**
 * Challenge Question and Response (challenge_q and challenge_r)
 */
%>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#BBE2EC">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[4] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#9FD5E3">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[4] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[4] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[4] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="48"
VALUE="<%= inputFieldReturnValues[4] %>">
<P>
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[5] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_OptionalLbl %>
<%= errorFlags[5] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[5] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="48"
VALUE="<%= inputFieldReturnValues[5] %>">
</TD>
</TR>
</TABLE>
```

Folgenden Code hinzu:

```
<% // Lo To Org Employee Information Begins %>
<P>
<TABLE WIDTH="580" BORDER="0" CELSPACING="2" CELLPADDING="10">
<TR>
<TD COLSPAN="2" ALIGN="LEFT" BGCOLOR="#336633">
<FONT SIZE="3" COLOR="#FFFFCC">
<STRONG>
LoTo Organization Employee Information
</STRONG>
</FONT>
</TD>
</TR>

<% // Employee Serial Number %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#EEEEAA">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[14] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#CCCC99">
```

```

<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[14] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[14] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[14] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="64"
VALUE="<%= inputFieldReturnValues[14] %>"
</TD>
</TR>

<% // Employee Job Title %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#EEEEAA">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[15] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#CCCC99">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[15] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[15] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[15] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="64"
VALUE="<%= inputFieldReturnValues[15] %>"
</TD>
</TR>

<% // Social Security Number %>
<TR>
<TD ALIGN="LEFT" BGCOLOR="#EEEEAA">
<FONT SIZE="2">
<%= STRING_InputFieldHelps[16] %>
</FONT>
</TD>
<TD ALIGN="LEFT" BGCOLOR="#CCCC99">
<FONT SIZE="2">
<STRONG>
<%= STRING_InputFieldLbls[16] %><%= STRING_Colon %>
</STRONG>
<%= STRING_Spacer %>
<%= STRING_RequiredLbl %>
<%= errorFlags[16] %>
</FONT>
<BR>
<INPUT TYPE="Text" NAME="<%= inputFieldNames[16] %>"
SIZE="<%= sizeOfInputFields %>"
MAXLENGTH="64"
VALUE="<%= inputFieldReturnValues[16] %>"
</TD>
</TR>
</TABLE>

```

Überprüfen persönlicher Daten

Im LoTo Organization-Beispiel wollen Sie prüfen können, ob Benutzer ihre persönlichen Informationen auf den Registrierungs-Web-Seiten im Browser eingeben. Auf den Browser-Registrierungs-Web-Seiten müssen Sie prüfen, ob die Felder für die laufende Mitarbeiternummer, den Jobtitel und die Versicherungsnummer ausgefüllt wurden.

Gehen Sie wie folgt vor, um zu prüfen, ob die Felder für die laufende Mitarbeiternummer, den Jobtitel und die Versicherungsnummer ausgefüllt wurden:

1. **In der Datei 'NSBrowserSSLCert_Enroll.jsp' müssen Sie unter folgendem Code-segment:**

```
<% // Missing E-mail Address Alert %>
<SCRIPT LANGUAGE="JavaScript">
<!--
function MissingEmailAddressAlert() {

var STRING_MissingEmailAddressPrompt = "Please enter your e-mail address.";

if ( document.RegForm.<%= emailNotificationFieldName %>.checked &&
document.RegForm.<%= inputFieldNames[3] %>.value == "" ) {
alert ( STRING_MissingEmailAddressPrompt );
document.RegForm.<%= inputFieldNames[3] %>.focus();
return true;
}
else {
return false;
}
}
//-->
</SCRIPT>
```

Folgenden Code hinzufügen:

```
<% // Missing Custom Info Alert %>
<SCRIPT LANGUAGE="JavaScript">
<!--
function MissingCustInfoAlert() {

var STRING_MissingCustInfoPrompt = "Please enter All the required fields";

if ( document.RegForm.<%= inputFieldNames[14] %>.value == "" ||
document.RegForm.<%= inputFieldNames[15] %>.value == "" ||
document.RegForm.<%= inputFieldNames[16] %>.value == "" ) {
alert ( STRING_MissingCustInfoPrompt );
document.RegForm.<%= inputFieldNames[14] %>.focus();
return true;
}
else {
return false;
}
}
//-->
</SCRIPT>
```

2. **Ändern Sie folgendes Segment:**

```
<% // If E-mail address is missing while e-mail notification is selected,
do not submit. %>
onSubmit="if ( MissingEmailAddressAlert() ) return false; else return true;">
```

In folgendes Segment:

```
<% // If E-mail address is missing while e-mail notification is selected,
do not submit. %>
onSubmit="if ( MissingEmailAddressAlert() ) return false;
else if ( MissingCustInfoAlert() )
return false; else return true;">
```

3. In der Datei 'NSBrowserSSLCert_Enroll.jsp' müssen Sie unter folgendem Code-segment:

```
var STRING_MissingEmailAddressPrompt = "Please enter your e-mail address.";

if ( document.RegForm.<%= emailNotificationFieldName %>.checked &&
document.RegForm.<%= inputFieldNames[3] %>.value == "" ) {
alert ( STRING_MissingEmailAddressPrompt );
document.RegForm.<%= inputFieldNames[3] %>.focus();
return true;
}
else {
return false;
}
}
//-->
</SCRIPT>
```

Folgenden Code hinzufügen:

```
<SCRIPT LANGUAGE="JavaScript">
<!--
function MissingCustInfoAlert() {

var STRING_MissingCustInfoPrompt = "Please enter All the required fields";

if ( document.RegForm.<%= inputFieldNames[14] %>.value == "" ||
document.RegForm.<%= inputFieldNames[15] %>.value == "" ||
document.RegForm.<%= inputFieldNames[16] %>.value == "" ) {
alert ( STRING_MissingCustInfoPrompt );
document.RegForm.<%= inputFieldNames[16] %>.focus();
return true;
}
else {
return false;
}
}
//-->
</SCRIPT>
```

4. Ändern Sie folgendes Segment:

```
CENTER>
<FORM NAME="SubmitBtnForm">
<INPUT TYPE="Button" NAME="submitBtn"
VALUE="<%= btnLbl %>"
onClick="
<% // E-mail address is missing while e-mail notification is selected. %>
if ( MissingEmailAddressAlert() ) return false;
<% // Generate PKCS #10 cert request and copy cert attributes to RegForm. %>
if ( ! CreatePKCS10CertReq() ) return false;
return true;
">
</FORM>
</CENTER>
```

In folgendes Segment:

```

CENTER>
<FORM NAME="SubmitBtnForm">
<INPUT TYPE="Button" NAME="submitBtn"
VALUE="<%= btnLbl %>"
onClick="
<% // E-mail address is missing while e-mail notification is selected. %>
if ( MissingEmailAddressAlert() ) return false;
<% // missing cust info %>
if ( MissingCustInfoAlert() ) return false;
<% // Generate PKCS #10 cert request and copy cert attributes to RegForm. %>
if ( ! CreatePKCS10CertReq() ) return false;
return true;
">
</FORM>
</CENTER>

```

Angeben der Seite, die nach dem Herunterladen des Zertifikats aufgerufen werden soll

Im LoTo Organization-Beispiel wollen Sie nach dem Herunterladen des Zertifikats zur Homepage des Unternehmens zurückkehren.

Gehen Sie wie folgt vor, um alle Dateien '*_Approve.jsp' entsprechend zu ändern:

1. Ändern Sie in der Datei '*_Approve.jsp' folgendes Codesegment:

```

<INPUT TYPE="button" VALUE="Return to Identitätsnachweis - Verwaltung"
onClick="top.location='
<%= PUBLIC_SERVER_URL_PATH%><% JSP_MOUNT_POINT %>
<% Page_Home %>'">

```

In folgendes Segment:

```

<INPUT TYPE="button" VALUE="Return to Company Web page"
onClick="top.location='http://mycompany.homepage.com'">

```

Grafiken ersetzen

Sie können die Grafikdateien in JSP-Dateien so ändern, dass auf Ihre Dateien verwiesen wird. Im vorliegenden Beispiel werden die folgenden Dateien durch angepasste GIF-Dateien ersetzt:

- SW_Banner.gif
- SW_Logo.gif
- TA_Banner.gif

Wechseln Sie von der generischen Datei:



Trust Authority

Zu einer angepassten Datei:



SVT Trust Authority Server

Aktualisieren des Benachrichtigungsbriefs

Sie können in E-Mail-Nachrichten den Namen des Unternehmens ändern.

Gehen Sie wie folgt vor, um den Namen des Unternehmens in E-Mails anzugeben:

1. **Ändern Sie in den 'Mail_*.ltr'-Dateien die Zeile:**

From: Tivoli PKI Certificate Enrollment

In folgende Zeile:

From: LoTo Organization Zertifikatsaussteller

Ändern von Zertifikatstypen

Sie können universelle Zertifikate mit einer Gültigkeitsdauer von einem oder zwei Jahren ausstellen, die den Web-Client, die E-Mail-Funktion sowie das digitale Unterzeichnen unterstützen und Browserzertifikatsoptionen ersetzen.

Serverzertifikatsseiten müssen nicht geändert werden.

1. Fügen Sie ein Zertifikatsprofil hinzu und aktivieren Sie die automatische Anforderungsverarbeitung.

Fügen Sie in der Datei 'certificate_profiles.cfg' unter folgendem Codesegment:

```
; --- S S L S E R V E R C E R T 2 Y E A R ---
[SSLServerCert2Year]
display_name=Web Server Authentication (2-Year)

; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,certificatePolicies
keyUsage=keyEncipherment&digitalSignature
extendedKeyUsage=serverAuth

; --- Define validityNotAfter values
validityNotAfter_range=0,730
validityNotAfter_default=730
```

Folgenden Code hinzu:

```
; --- Universal C e r t 1 Y e a r ---
[UniversalCert]
display_name=Universal Certificate
required_fields=first_name,last_name,email_address

; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,subjectAltName,certificatePolicies
keyUsage=digitalSignature&keyEncipherment
extendedKeyUsage=emailProtection,clientAuth
subjectAltName=rfc822Name=%MAIL%
; --- Define validityNotAfter values
validityNotAfter_range=0,365
validityNotAfter_default=365

; --- Auto: approve or pend
decision_default=approve

; --- renewable: true or false
credential_renewable=true
```

2. Ändern Sie den Anzeigenamen eines Zertifikatstyps.

Ändern Sie in der Datei 'certificate_profiles.cfg' folgendes Codesegment:

```
; --- S / M I M E C e r t 2 Y e a r ---
[S/MIMECert2Year]
display_name=E-mail Protection (2-Year)
required_fields=first_name,last_name,email_address
```

In folgendes Segment:

```
; --- S / M I M E C e r t 2 Y e a r ---
[S/MIMECert2Year]
display_name=Universal (2-Year)
required_fields=first_name,last_name,email_address
```

3. Ändern Sie ein Zertifikatsprofil.

Ändern Sie in der Datei 'certificate_profiles.cfg' folgendes Codesegment:

```
; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,subjectAltName,certificatePolicies
keyUsage=digitalSignature&keyEncipherment
extendedKeyUsage=emailProtection
subjectAltName=rfc822Name=%MAIL%
```

In folgendes Segment:

```
; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,subjectAltName,certificatePolicies
keyUsage=digitalSignature&keyEncipherment
extendedKeyUsage=emailProtection,clientAuth
subjectAltName=rfc822Name=%MAIL%
```

4. Löschen Sie ein Zertifikatsprofil.

Löschen Sie in der Datei 'certificate_profiles.cfg' den folgenden Code:

```
; --- S S L B R O W S E R C E R T 2 Y E A R ---
[SSLBrowserCert2Year]
display_name=Web Client Authentication (2-Year)

; --- Define Extensions
extensions_required=keyUsage,extendedKeyUsage,certificatePolicies
keyUsage=digitalSignature
extendedKeyUsage=clientAuth

; --- Define validityNotAfter values
validityNotAfter_range=0,730
validityNotAfter_default=730
```

Anmerkung: Beim Hinzufügen oder Löschen von Zertifikatsprofilen müssen Sie die RA Desktop-Konfigurationsdatei 'raprofiles.cfg' so ändern, dass die gewünschten Zertifikatsprofile dort entweder definiert oder nicht definiert sind. Andernfalls kann RA Desktop aufgrund einer Nullzeiger-Ausnahmebedingung nicht initialisiert werden.

Ändern Sie in der Datei 'raprofiles.cfg' folgendes Codesegment:

```
RequestProfiles=S/MIMECert1Year,
S/MIMECert2Year,
IPSecCert1Year,
IPSecCert2Year,
SSLServerCert1Year,
SSLServerCert2Year,
SSLBrowserCert2Year,
SSLBrowserCert1Year,
SignatureOnlyCert1Year,
SignatureOnlyCert2Year,
KeyEnciphermentCert2Year,
KeyEnciphermentCert1Year,
DataEnciphermentCert1Year,
DataEnciphermentCert2Year,
NonRepudiationCert2Year,
NonRepudiationCert1Year,
CACrossCertificationRequest
```

In folgendes Segment:

```
RequestProfiles=S/MIMECert1Year,
S/MIMECert2Year,
IPSecCert1Year,
IPSecCert2Year,
SSLServerCert1Year,
SSLServerCert2Year,
UniversalCert,
SSLBrowserCert1Year,
SignatureOnlyCert1Year,
SignatureOnlyCert2Year,
KeyEnciphermentCert2Year,
KeyEnciphermentCert1Year,
DataEnciphermentCert1Year,
DataEnciphermentCert2Year,
NonRepudiationCert2Year,
NonRepudiationCert1Year,
CACrossCertificationRequest
```

Hinzufügen von Werten zu Auswahllisten

Sie können Werte zu einer Auswahlliste hinzufügen, die auf einer Registrierungswebseite angezeigt wird. Wählen Sie Dateinamen aus, die für den Betrieb verwendet werden.

Gehen Sie wie folgt vor:

1. Stoppen Sie Tivoli PKI.
2. Fügen Sie einen Wert zu der Auswahlliste hinzu, die auf einer Registrierungs-Web-Seite angezeigt wird. Ähnlich wie der Abschnitt zu den Zertifikatstypen müssen auch die neuen Zertifikatsprofile in der Datei 'Mycertificate_profiles.cfg' vordefiniert werden.

Ändern Sie in der Datei 'raconfig.cfg' folgendes Codesegment:

```
CertProfiles_NSBrowserSSLCert=SSLBrowserCert1Year,SSLBrowserCert2Year,
S/MIMECert1Year,S/MIMECert2Year CertProfiles_IEBrowserSSLCert=SSLBrowserCert1Year,
SSLBrowserCert2Year,
S/MIMECert1Year,S/MIMECert2Year
```

In folgendes Segment:

```
CertProfiles_NSBrowserSSLCert=UniversalCert,S/MIMECert2Year
CertProfiles_IEBrowserSSLCert=UniversalCert,S/MIMECert2Year
```

3. Wählen Sie Dateinamen aus, die für den Betrieb verwendet werden. **Ändern Sie in der Datei 'raconfig.cfg' folgendes Codesegment:**

```
Page_Enroll_NSBrowserSSLCert=NSBrowserSSLCert_Enroll.jsp
Page_Enroll_IEBrowserSSLCert=IEBrowserSSLCert_Enroll.jsp
CertificateProfiles=/usr/lpp/iau/pkrf/Domains/LoTo/etc/certificate_profiles.cfg
```

In folgendes Segment:

```
Page_Enroll_NSBrowserSSLCert=MyNSBrowserSSLCert_Enroll.jsp
Page_Enroll_IEBrowserSSLCert=MyIEBrowserSSLCert_Enroll.jsp
CertificateProfiles=/usr/lpp/iau/pkrf/Domains/LoTo/etc/Mycertificate_profiles.cfg
```

4. Starten Sie Tivoli PKI.

Verarbeiten von Genehmigungen

Regel-Exits ermöglichen durch das Anpassen der Registrierungsprozesse die automatische Verarbeitung von Genehmigungen. Die Regel-Exits können zur Ausführung der folgenden Aktionen aufgerufen werden:

- Browser-SSL-Zertifikatsregistrierungsanforderungen
- Browser-SSL-Zertifikatserneuerungsanforderungen
- PKCS #10- und PKCS #7-Zertifikatsregistrierungsanforderungen
- Vom Endbenutzer eingeleitete Widerrufsanforderungen
- Vorabregistrierungsanforderungen
- Nach der Ausstellung eines Zertifikats an einen Client
- Während den von RA Desktop eingeleiteten Aktionen (Genehmigung, Zurückweisung, Zurückstellung und Widerruf)

Tivoli PKI stellt den Beispiel-Regel-Exit 'auto_approve' zur Verfügung, mit dem alle Zertifikatsanforderungen genehmigt werden können, für die in der Datei 'certificate_profile-s.cfg.' der Wert 'decision_default=approve' angegeben wurde. Der Regel-Exit 'auto_approve' kann so angepasst oder umgeschrieben werden, dass zusätzliche Verarbeitungsoperationen ausgeführt werden können. Hierzu gehört z. B. das Prüfen des Identitätsnachweises und/oder der Berechtigung eines Benutzers für den angeforderten Zertifikatstyp durch die interaktive Kommunikation mit anderen Anwendungen oder Services innerhalb des Unternehmens. Bei dem Beispiel-Regel-Exit kann es sich um eine in einer beliebigen Programmiersprache geschriebene Komponente wie beispielsweise eine C++- oder Shell-Komponente etc. handeln.

Die folgenden Schritte illustrieren ein Szenario, bei dem allen Mitgliedern, deren automatische Genehmigung angefordert wurde, die Werte '/O=BUGS/OU=ITS /O=TWT/OU=DEV' zugeordnet wurden.

1. Ändern Sie den zum Programmpaket von Tivoli PKI gehörigen Beispiel-Regel-Exit 'auto_approve' entsprechend Ihren Anforderungen:

- a. **Ändern Sie in der Datei 'auto_approve.cpp' die folgende Zeile:**

```
const char* decision_default = bpvars.findVariable("decision_default");
```

In folgenden Code:

```
const char* decision_default = bpvars.findVariable("decision_default");
const char* OU =
bpvars.findVariable("OU");
const char* O = bpvars.findVariable("O");
```

- b. **Ändern Sie in der Datei 'auto_approve.cpp' folgendes Codesegment:**

```
if ( strstr(decision_default, "approve") ) {
cerr << now << "Request is Approved\n";
response.addVariable("reqStatus", "Approved");
}
```

In folgendes Segment:

```
if ( (strstr(decision_default, "approve")) || ( (strcmp(O,"BUGS")==0) &&
(strcmp(OU,"ITS")==0) ) || ( (strcmp(O,"TWT")==0) && (strcmp(OU,"DEV")==0))) {
cerr << now << "Request is Approved\n";
response.addVariable("reqStatus", "Approved");
}
```

2. Kompilieren Sie die Datei 'auto_approve.cpp'.
3. Kopieren Sie die ausführbare Datei des Regel-Exits an die selbe Position, an der die bereits installierte, ausführbare Datei gespeichert ist. Beispiel: Unter AIX - /usr/lpp/iau/pkrf/Domains/*YourDomain*/bin. Unter Windows NT - C:\Program Files\IBM\Tivoli PKI\pkrf\Domains*YourDomain*\bin.
4. Wenn der Name der ausführbaren Datei vom Standardwert abweicht, müssen Sie alle zugehörigen Einträge in der Datei 'raconfig.cfg' folgendermaßen ändern:
`afservice.PolicyExit=com.ibm.irg.ra.afw.services.SpawnPolicyExitLongRunningFactory,
installationspfad\name_des_angepassten_programms`
5. Stoppen Sie Tivoli PKI und führen Sie anschließend einen Neustart durch.

Verzeichnis-Server anpassen

Während der Installation von Tivoli PKI wird nur der CA-Knoten erstellt. Wenn ein Zertifikat angefordert wird, kann die Registrierungsstelle (RA) nur die Blattkomponente des Eintrags erstellen. Die Knoteneinträge müssen im Verzeichnis (Directory) bereits definiert sein. Beispiel: Wenn die Registrierungsstelle den Eintrag '/C=US/O=BUGS/OU=ITS/CN=User1' erstellen will, müssen die Einträge für 'C=US', 'O=BUGS' und 'OU=ITS' bereits vorhanden sein. Wird ein Zertifikat angefordert, bei dem die zugehörigen Knoteneinträge nicht vorhanden sind, gibt die Registrierungsfunktion von Tivoli PKI ein Zertifikat an den Antragsteller zurück. Das Zertifikat wird nicht im Verzeichnis (Directory) gespeichert und kann deswegen auch nicht gesucht oder abgerufen werden.

Die folgenden Schritte beschreiben das Anpassen eines Verzeichnis-Servers an die innerhalb des Unternehmens geltende Hierarchie:

1. Stoppen Sie Tivoli PKI.
2. Editieren Sie mit einem beliebigen Texteditor die Datei 'slapd.conf'.

Für AIX:

/usr/ldap/etc/slapd.conf

Für Windows NT:

c:\Program Files\IBM\ldap\etc\slapd.conf

3. Suchen Sie in der Datei nach folgender Zeile:

suffix "cn=localhost" suffix "cn=US"

Fügen Sie direkt nach dieser Zeile die folgende Zeile ein:

suffix "c=country code"

Hierbei steht *country code* für den Code eines bestimmten Landes. Beispiel:

suffix "c=ES" suffix "c=GB"

4. Starten Sie Tivoli PKI.
5. Erstellen Sie eine Datei mit allen Einträgen, die zum Verzeichnisserver hinzugefügt werden müssen, z. B. 'ldapadd.txt'.

-
6. Führen Sie den folgenden Befehl in dem Verzeichnis aus, in dem 'ldapadd.txt' gespeichert ist:

```
ldapadd -D "<Ldap Root DN>" -w "<Ldap Root DN Password>" -c -f ldapadd.txt
```

Hierbei steht <Ldap Root DN> für den registrierten Namen des Roots für LDAP und <Ldap Root DN Password> für das zugehörige Kennwort.

7. Stellen Sie sicher, dass alle Einträge korrekt hinzugefügt werden.
8. Fügen Sie mit dem Befehl **ldapadd** alle weiteren Einträge hinzu.
9. Melden Sie sich als LDAP-Root an.
10. Erstellen Sie mit DMT (Directory Management Tool) die korrekten Zugriffssteuerungslisten (ACLs) für alle neuen Knoten von DirAdmin.
11. Melden Sie sich als LDAP-Root an und erstellen Sie mit DMT die korrekten Zugriffssteuerungslisten (ACLs) für alle neu erstellten Knoten.

Anpassen von Objektklassen für Verzeichniseinträge (Directory)

Während der Tivoli PKI-Registrierung wird das Zertifikat für das Verzeichnis (Directory) publiziert. Das Verzeichnis enthält alle vom CA-Server erstellten Zertifikate in hierarchischer Reihenfolge. Die Hierarchie basiert auf den Attributen, die in den RDNs des Zertifikatsgegenstands enthalten sind. Tivoli PKI unterstützt eine begrenzte Gruppe von Attributen, die als Teil des Namens des Zertifikatsgegenstands (subjectName) verwendet werden können. Jede RDN wird im Verzeichnis als ein Eintrag dargestellt, und die Eintragsart basiert auf den Attributen, aus denen sich die RDN zusammensetzt. Unter Tivoli PKI können Sie definieren, welche Objektklasse beim Erstellen von Verzeichniseinträgen für die bestimmten RDNs verwendet werden soll. Allerdings muss Ihre Definition mit dem Verzeichnisschema kompatibel sein.

Jede Eintragsart (Objektklasse) verfügt über eine Schemadefinition, die beschreibt, welche Attribute beim Erstellen eines Eintrags der betreffenden Art optional und welche Attribute erforderlich sind. Für einen Eintrag können mehrere Objektklassen verwendet werden, solange es sich nur bei einer Objektklasse um eine strukturelle Objektklasse ('structural') handelt. Beispiel: Für ein Zertifikat namens '/C=US/O=BUGS/OU=ITS/CN=User' könnte der Benutzer die RDN '/CN=User' mit einer anderen Objektklasse erstellen.

Im Folgenden wird beschrieben, wie der Eintrag angepasst wird:

1. Editieren Sie die Datei 'certificate_profiles.cfg' im Verzeichnis '/usr/lpp/iau/pkrf/domains/Your_Domain_Name/etc', wobei *Your_Domain_Name* der Name Ihrer Domäne ist.
2. Suchen Sie die Objektklassendefinition für das CN-Attribut.

Anmerkung: Einigen Werten ist unter Umständen keine Definition zugeordnet. Liegen keine Definitionen vor, muss der Benutzer Definitionen angeben, wenn eine Anpassung erforderlich ist.

```

; --- Object Class to be used to create entries on Directory that have the following
attribute.
; --- (Definitions will be provided by adding variable name x_objectclass, where "x"
; --- is the RDN name.)
; --- Object Class has to match a object class on the directory schema.
; --- Required Attributes refer to values required to add the entry to the directory.
; --- Optional Attributes refer to values that could be used on the creation of the entry if
; --- available on enrollment data.

```

```

; --- Example configuration if going to use different schema.
;CN_objectClass=inetOrgPerson,ePerson,top
;CN_objectClass_RequiredAttributes=cnAttr,snAttr
;CN_objectClass_OptionalAttributes=

```

3. Ändern Sie die Definition so, dass sie dem gewünschten Schema entspricht:

```

CN_objectClass=pkiUser,top
CN_objectClass_RequiredAttributes=cnAttr
CN_objectClass_OptionalAttributes=

```

Anmerkung: Die ausgewählten Objektklassen müssen in der Schemadefinition das optionale Attribut 'userCertificate' enthalten.

4. Integrieren Sie die Definition der Attribute, die in Ihrer Objektklassendefinition enthalten sind.

```

; --- Describes the values on the enrollment data to be used to populate the information
; --- on the directory.
; --- The AttributeNames need to match the attribute name specified on the directory schema.
; --- The subjectName object refers to the attribute values found on the entry RDN.

```

```

cnAttr_AttributeValue=%subjectName.CN%
cnAttr_AttributeFormat=String
cnAttr_AttributeName=cn

```

Änderungen prüfen

Prüfen Sie die Funktionen von Tivoli PKI, indem Sie die folgenden Aufgaben ausführen:

- Browser-basierte Zertifikate mit Netscape registrieren.
- Browser-basierte Zertifikate mit Microsoft Internet Explorer registrieren.
- Browser-basierte Zertifikate mit Netscape erneuern.
- Browser-basierte Zertifikate mit Microsoft Internet Explorer erneuern.
- Browser-basierte Zertifikate mit Netscape widerrufen.
- Browser-basierte Zertifikate mit Microsoft Internet Explorer widerrufen.
- Server-basierte Zertifikate mit Netscape registrieren.
- Server-basierte Zertifikate mit Microsoft Internet Explorer registrieren.
- Vorabregistrierung mit Netscape aufrufen.
- Vorabregistrierung mit Microsoft Internet Explorer aufrufen.
- RA Desktop konfigurieren und die Funktionen zum Genehmigen, Widerrufen, Zurückstellen und Zurückweisen testen.

Glossar

In diesem Glossar werden alle Termini und Abkürzungen definiert, die in diesem Handbuch verwendet werden und die möglicherweise neu oder unbekannt und von Bedeutung sind.

Numerische Einträge

4758 PCI Cryptographic Coprocessor

Eine programmierbare, manipulationssensitive PCI-Bus-Verschlüsselungskarte, die die Ausführung von DES- und RSA-Verschlüsselungsoperationen mit hoher Geschwindigkeit ermöglicht. Die Verschlüsselungsprozesse werden in einem gesicherten und abgegrenzten Bereich auf der Karte ausgeführt. Die Karte entspricht den strengen Anforderungen des FIPS PUB 140-1 Level 4-Standards. In dem gesicherten und abgegrenzten Bereich kann Software ausgeführt werden. Der SET-Standard kann z. B. zur Verarbeitung von Kreditkartentransaktionen genutzt werden.

A

Abstract Syntax Notation One (ASN.1)

Eine ITU-Notation, die zum Definieren der Syntax von Informationsdaten benutzt wird. Sie definiert eine Reihe einfacher Datentypen und gibt eine Notation für die Identifizierung dieser Typen und die Angabe von Werten für diese Typen an. Diese Notationen können verwendet werden, wenn es erforderlich ist, die abstrakte Syntax von Informationen zu definieren, ohne damit die Art der Verschlüsselung dieser Informationen für die Übertragung zu beeinträchtigen.

ACL

Access Control List - Zugriffssteuerungsliste.

Aktionsprotokoll

Die Aufzeichnung aller Ereignisse, die während der gesamten Gültigkeitsdauer eines Identitätsnachweises aufgetreten sind.

American National Standard Code for Information Interchange (ASCII)

Der Standardcode, der für den Austausch von Informationen zwischen Datenverarbeitungssystemen, DFV-Systemen und zugehöriger Hardware verwendet wird. ASCII verwendet einen codierten Zeichensatz, der aus Zeichen von 7 Bit Länge (bzw. 8 Bit bei Paritätsprüfung) besteht. Der Zeichensatz besteht hierbei aus Steuerzeichen und Schriftzeichen.

American National Standards Institute (ANSI)

Eine Organisation, die die Verfahrensweisen definiert, mit deren Hilfe akkreditierte Organisationen freiwillig eingehaltene Industriestandards in den Vereinigten Staaten festlegen und verwalten. Ihr gehören Hersteller, Verbraucher und allgemeine Interessenvertretungen an.

Anforderungs-ID

Ein aus 24 bis 32 Zeichen bestehender ASCII-Wert, der zur eindeutigen Identifikation einer Zertifikatsanforderung gegenüber der RA dient. Dieser Wert kann bei der Transaktion für die Zertifikatsanforderung verwendet werden, um den Status der Anforderung oder des zugehörigen Zertifikats abzurufen.

ANSI

American National Standards Institute.

Applet

Ein in der Programmiersprache Java geschriebenes Computerprogramm, das innerhalb eines Java-kompatiblen Webbrowsers ausgeführt werden kann. Wird auch als Java-Applet bezeichnet.

Art

Siehe Objektart.

ASCII

American National Standard Code for Information Interchange.

ASN.1

Abstract Syntax Notation One.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsverfahren, das zur Ver- und Entschlüsselung unterschiedliche, asymmetrische Schlüssel verwendet. Jedem Benutzer wird hierbei ein Schlüsselpaar zugeordnet, das einen allgemeinen, für alle zugänglichen Schlüssel und einen privaten Schlüssel umfasst, der nur dem jeweiligen Benutzer bekannt ist. Eine gesicherte Transaktion kann ausgeführt werden, wenn der öffentliche Schlüssel sowie der zugehörige private Schlüssel übereinstimmen. In diesem Fall kann die Transaktion entschlüsselt werden. Dieses Verfahren wird auch als Verschlüsselung auf der Basis von Schlüsselpaaren bezeichnet. *Gegensatz zu* Symmetrische Verschlüsselung.

Asynchrone Übertragung

Ein Übertragungsmodus, bei dem Sender und Empfänger nicht gleichzeitig vorhanden sein müssen.

Authentifizierung

Der Vorgang, bei dem die Identität eines Teilnehmers an einer Übertragung zuverlässig überprüft wird.

B**Base64-Verschlüsselung**

Ein häufig verwendetes Verfahren bei der Übertragung von Binärdaten mit MIME.

Basic Encoding Rules (BER)

Die Regeln, die in ISO 8825 für die Verschlüsselung von in ASN.1 beschriebenen Dateneinheiten angegeben sind. Die Regeln geben das Verschlüsselungsverfahren, jedoch nicht die abstrakte Syntax an.

Benutzerauthentifizierung

Der Prozess, mit dem überprüft wird, ob der Absender einer Nachricht die berechtigte Person ist, als die er sich ausgibt. Der Prozess überprüft außerdem, ob ein Kommunikationsteilnehmer auch tatsächlich mit dem erwarteten Endbenutzer oder System in Verbindung steht.

BER

Basic Encoding Rules.

Berechtigung

Die Erlaubnis, auf eine Ressource zuzugreifen.

Bestreiten

Etwas als unwahr zurückweisen. Dies ist z. B. dann der Fall, wenn ein Benutzer abstreitet, eine bestimmte Nachricht gesendet oder eine bestimmte Anforderung übergeben zu haben.

Browser

Siehe Web-Browser.

Browser-Zertifikat

Ein digitales Zertifikat, das auch als Zertifikat der Client-Seite bezeichnet wird. Es wird von einem CA über einen für SSL aktivierten Web-Server ausgestellt. Die Schlüssel in einer verschlüsselten Datei ermöglichen dem Inhaber des Zertifikats das Verschlüsseln, Entschlüsseln und Unterzeichnen von Daten. Normalerweise werden diese Schlüssel im Web-Browser gespeichert. In bestimmten Anwendungen können die Schlüssel auf Smart-Cards oder anderen Speichermedien gespeichert werden. *Siehe auch* Digitales Zertifikat.

Bytecode

Maschinenunabhängiger Code, der mit dem Java-Compiler generiert und mit dem Java-Interpreter ausgeführt wird.

C**CA**

Certificate Authority - Zertifikatsaussteller.

CA-Hierarchie

Bei Tivoli PKI eine Sicherungsstruktur, bei der ein CA auf der höchsten Ebene positioniert ist. Anschließend können bis zu vier weitere Ebenen mit untergeordneten CAs definiert werden. Wenn Benutzer oder Server bei einem

Zertifikatsaussteller registriert werden, wird ihnen ein von diesem Aussteller unterzeichnetes Zertifikat zugeordnet. Außerdem übernehmen sie die Zertifizierungshierarchie der übergeordneten Ebenen.

CA-Server

Der Server für die CA-Komponente von Tivoli PKI.

CAST-64

Ein Block-Cipher-Algorithmus, der mit einer Blockgröße von 64 Bit und einem 6-Bit-Schlüssel arbeitet. Er wurde von Carlisle Adams und Stafford Tavares entwickelt.

CA-Zertifikat

Ein Zertifikat, das vom Web-Browser eines Benutzers auf dessen Anforderung hin von einem nicht identifizierten CA akzeptiert wird. Der Browser kann dann dieses Zertifikat verwenden, um für die Kommunikation mit Servern, die über Zertifikate dieses CAs verfügen, eine Authentifizierung durchzuführen.

CCA

IBM Common Cryptographic Architecture.

CDSA

Common Data Security Architecture.

CGI

Common Gateway Interface.

Client

(1) Eine Funktionseinheit, die gemeinsam benutzte Services von einem Server empfängt. (2) Ein Computer oder Programm, der/das Services von einem anderen Computer oder Programm anfordert.

Client/Server

Ein Modell für die verteilte Verarbeitung, bei dem ein Programm an einem Standort eine Anforderung an ein Programm an einem anderen Standort sendet und auf eine Antwort wartet. Das anfordernde Programm wird als Client, das antwortende als Server bezeichnet.

Codeunterzeichnung

Ein Verfahren zum Unterzeichnen ausführbarer Programme mit einer digitalen Unterschrift. Die Codeunterzeichnung dient zur Verbesserung der Zuverlässigkeit von Softwarekomponenten, die über das Internet verteilt werden.

Common Cryptographic Architecture (CCA)

IBM Software, die einen konsistenten Verschlüsselungsansatz auf den wichtigsten IBM Computerplattformen bietet. Sie unterstützt Anwendungssoftware, die in einer Vielzahl von Programmiersprachen geschrieben wurde. Die Anwendungssoftware kann hierbei die CCA-Services aufrufen, um eine breite Palette kryptografischer Funktionen (einschließlich der DES- und der RSA-Verschlüsselung) auszuführen.

Common Data Security Architecture (CDSA)

Eine Initiative zum Definieren eines umfassenden Ansatzes für Sicherheitsservices und Sicherheitsverwaltungsoperationen bei computerbasierten Sicherheitsanwendungen. Diese Architektur wurde von Intel entworfen und dient dazu, Computerplattformen für Anwendungen sicherer zu gestalten.

Common Gateway Interface (CGI)

Ein Standardverfahren zum Übertragen von Informationen zwischen Web-Seiten und Webservern.

CRL

Certificate Revocation List - Zertifikatswiderrufsliste.

CRL-Publikationsintervall

Dieses Intervall wird in der CA-Konfigurationsdatei definiert und gibt das Zeitintervall zwischen zwei Publikationen der Zertifikatswiderrufsliste im Directory an.

D

Dämon

Ein Programm, das Tasks im Hintergrund ausführt. Es wird implizit aufgerufen, wenn eine Bedingung auftritt, die die Hilfe des Dämons erforderlich macht. Es ist nicht erforderlich, dass der Benutzer über die Ausführung des Dämons unterrichtet wird, da der Dämon normalerweise vom System automatisch gestartet wird. Ein Dämon kann über eine unbegrenzte Zeit hinweg ausgeführt oder vom System in bestimmten Zeitintervallen erneut generiert werden.

Der Terminus (englisch *demon*) stammt aus der Mythologie. Später wurde er aber als Akronym für den Ausdruck "Disk And Execution MONitor" (Platten- und Ausführungsüberwachungsprogramm) erklärt.

Data Encryption Standard (DES)

Eine Verschlüsselungs-Block-Cipher, die 1977 von der US-Regierung als offizieller Standard definiert und übernommen wurde. Dieser Standard wurde ursprünglich von IBM entwickelt. DES wurde seit seiner Veröffentlichung umfassend untersucht und stellt ein allgemein bekanntes und häufig verwendetes Verschlüsselungssystem zur Verfügung.

Bei DES handelt es sich um ein symmetrisches Verschlüsselungssystem. Um es für die Datenübertragung einzusetzen, müssen sowohl der Sender als auch der Empfänger den selben, geheimen Schlüssel kennen. Dieser Schlüssel wird zum Ver- und Entschlüsseln der Nachricht verwendet. DES kann außerdem zur Durchführung von Verschlüsselungsoperationen für einzelne Benutzer eingesetzt werden, z. B. zum Speichern von verschlüsselten Dateien auf einer Festplatte. DES arbeitet mit einer Blockgröße von 64 Bit und verwendet für die Verschlüsselung einen 56-Bit-Schlüssel. Ursprünglich wurde dieser Standard für die Hardwareimplementierung entwickelt. DES wird von NIST alle fünf Jahre erneut als offizieller Verschlüsselungsstandard der US-Regierung zertifiziert.

Datenspeicherbibliothek (DL)

Ein Modul, das den Zugriff auf permanente Datenspeicher mit Zertifikaten, CRLs, Schlüsseln, Regeln und anderen sicherheitsrelevanten Objekten ermöglicht.

DEK

Document Encryption Key = Dokumentverschlüsselungsschlüssel.

DER

Distinguished Encoding Rules.

DES

Data Encryption Standard.

Diffie-Hellman

Ein Verfahren zur Datenverschlüsselung, das auf der Verwendung eines gemeinsamen Schlüssels auf einem nicht gesicherten Medium basiert und nach seinen Erfindern (Whitfield Diffie und Martin Hellman) benannt wurde.

Digitales Zertifikat

Ein elektronischer Identitätsnachweis, der von einer zuverlässigen Stelle für eine Person oder Entität ausgestellt wird. Jedes Zertifikat ist mit dem privaten Schlüssel des CAs unterzeichnet. Es bürgt für die Identität einer Person, eines Unternehmens oder einer Organisation.

Abhängig vom Aufgabenbereich des CAs kann das Zertifikat die Berechtigung seines Inhabers bestätigen, e-Business-Transaktionen über das Internet auszuführen. In gewisser Weise hat ein digitales Zertifikat eine ähnliche Funktion wie ein Führerschein oder ein Meisterbrief. Es bestätigt, dass der Inhaber des entsprechenden privaten Schlüssels berechtigt ist, bestimmte e-Business-Aktivitäten auszuführen.

Ein Zertifikat enthält Informationen über die Entität, die von ihm zertifiziert wird, gibt an, ob es sich um eine Person, eine Maschine oder ein Computerprogramm handelt und enthält als Teil dieser Informationen den zertifizierten öffentlichen Schlüssel dieser Entität.

Digitale Unterschrift

Eine codierte Nachricht, die an Dokumente oder Daten angefügt wird, und die Identität des Absenders nachweist. Eine digitale Unterschrift gewährleistet ein höheres Maß an Sicherheit als eine physische Unterschrift, da es sich hierbei nicht lediglich um einen verschlüsselten Namen oder eine Reihe einfacher Identifikationscodes handelt.

Eine digitale Unterschrift enthält eine verschlüsselte Zusammenfassung der unterzeichneten Nachricht. Durch das Anfügen einer digitalen Unterschrift an eine Nachricht lässt sich der Absender also zweifelsfrei feststellen. (Die Unterschrift kann nur mit Hilfe des Schlüssels des Absenders erstellt werden.) Außerdem ermöglicht sie die Absicherung des Inhalts der unterzeichneten Nachricht, da die verschlüsselte Nachrichtenzusammenfassung mit dem Nachrichteninhalt übereinstimmen muss. Andernfalls wird die Unterschrift nicht als gültig identifiziert. Eine digi-

tale Unterschrift kann also nicht von einer Nachricht kopiert und für eine andere Nachricht verwendet werden, da sonst die Zusammenfassung (Hash-Code) nicht übereinstimmen würde. Alle Änderungen an der unterzeichneten Nachricht führen automatisch zum Verlust der Gültigkeit der Unterschrift.

Digitale Zertifizierung

Siehe Zertifizierung.

Digital Signature Algorithm (DSA)

Ein auf öffentlichen Schlüsseln basierender Algorithmus, der zum Standard für digitale Unterschriften (Digital Signature Standard = DSS) gehört. Er kann nur für digitale Unterschriften, jedoch nicht für die Verschlüsselung verwendet werden.

Directory

Eine hierarchische Struktur, die als globales Repository für Informationen zur Datenkommunikation (wie beispielsweise E-Mail oder Austausch von verschlüsselten Daten) konzipiert ist. Im Directory werden bestimmte Elemente gespeichert, die für die PKI-Struktur (PKI = Public Key Infrastructure) unbedingt erforderlich sind. Hierzu gehören die folgenden Elemente: öffentliche Schlüssel, Zertifikate und Zertifikatswiderrufslisten (CRLs).

Die Daten im Directory sind hierarchisch in einer Baumstruktur organisiert, wobei die oberste Ebene der Baumstruktur das Root-Verzeichnis ist. Häufig stehen Organisationen einer höheren Ebene für einzelne Länder, Regierungen oder Unternehmen. Benutzer oder Einheiten werden im Allgemeinen als "Blätter" einer solchen Baumstruktur dargestellt. Diese Benutzer, Organisationen, Standorte, Länder und Einheiten haben jeweils ihren eigenen Eintrag. Jeder Eintrag besteht aus Attributen, denen verschiedene Typen zugewiesen sind. Diese enthalten Informationen zu den Objekten, für die der jeweilige Eintrag steht.

Jeder Eintrag im Directory ist mit einem zugeordneten registrierten Namen (DN = Distinguished Name) verbunden. Dieser ist eindeutig, wenn der Eintrag ein Attribut umfasst, das für das tatsächliche Objekt als eindeutig bekannt ist. Im folgenden DN-Beispiel wurde als Land (C = Country) US, als Unternehmen (O = Organization) IBM, als Unternehmenseinheit (OU = Organization Unit) Trust und als allgemeiner Name (CN = Common Name) der Wert CA1 angegeben.

C=US/O=IBM/OU=Trust/CN=CA1

Directory-Server

In Tivoli PKI das IBM Directory. Dieses Directory unterstützt die LDAP-Standards und verwendet DB2 als Basissystem.

Distinguished Encoding Rules (DER)

Durch DER werden bestimmte Einschränkungen für BER definiert. Mit DER kann genau ein bestimmter Verschlüsselungstyp aus den verfügbaren und auf der Basis der Verschlüsselungsregeln als zulässig definierten Typen ausgewählt werden. Hierdurch werden alle Senderoptionen eliminiert.

DL

Data Storage Library = Datenspeicherbibliothek.

DN

Distinguished Name - Registrierter Name.

Dokumentverschlüsselungsschlüssel (DEK)

Normalerweise ein symmetrischer Ver-/Entschlüsselungsschlüssel, z. B. DES.

Domäne

Siehe Sicherheitsdomäne und Registrierungsdomäne.

DSA

Digital Signature Algorithm.

E

e-Business

Das Durchführen geschäftlicher Transaktionen über Netze und Computer, z. B. der Kauf und Verkauf von Waren und Dienstleistungen sowie der Transfer von Zahlungsmitteln mit Hilfe der digitalen Kommunikation.

e-Commerce

Unternehmensübergreifende Transaktionen wie beispielsweise der Kauf und Verkauf von Waren und Dienstleistungen (zwischen Unternehmen und ihren Kunden, Lieferanten, Subunternehmen und anderen) über das Internet. E-Commerce stellt einen Kernbestandteil des e-Business dar.

Endentität

Der Gegenstand eines Zertifikats, bei dem es sich nicht um einen CA handelt.

Entschlüsseln

Den Verschlüsselungsprozess rückgängig machen.

Exemplar

Bei DB2 bezeichnet man als Exemplar eine logische Datenbankverwaltungsumgebung zum Speichern von Daten und Ausführen von Anwendungen. Es ermöglicht die Definition einer allgemeinen Gruppe von Konfigurationsparametern für verschiedene Datenbanken.

Extranet

Ein Netz, das auf dem Internet basiert und eine ähnliche Technologie einsetzt. Unternehmen beginnen momentan mit dem Einsatz des Web Publishings, elektronischen Handels und der Nachrichtenübertragung sowie der Verwendung von Groupware für verschiedene Gruppen von Kunden, Partnern und internen Mitarbeitern.

F

File Transfer Protocol (FTP)

Ein Client/Server-Protokoll im Internet, das zum Übertragen von Dateien zwischen Computern benutzt wird.

Firewall

Ein Gateway zwischen Netzen, der den Informationsfluss zwischen diesen einschränkt. Normalerweise dienen Firewalls dem Schutz interner Netze gegen die nicht berechnigte Verwendung durch externe Personen.

FTP

File Transfer Protocol.

G

Gateway

Eine Funktionseinheit, mit deren Hilfe nicht kompatible Netze oder Anwendungen Daten austauschen können.

Gegenseitige Zertifizierung

Ein Trust-Modell, bei dem ein CA für einen anderen CA ein Zertifikat ausstellt, das den öffentlichen Schlüssel enthält, der dem entsprechenden privaten Unterschriftsschlüssel zugeordnet ist. Ein gegenseitig zertifiziertes Zertifikat ermöglicht Client-Systemen oder Endentitäten in einer Verwaltungsdomäne die sichere Kommunikation mit Client-Systemen oder Endentitäten in einer anderen Domäne.

Gesicherte Computerbasis (TCB)

Die Software- und Hardwareelemente, die zur Umsetzung der Computersicherheitsregeln eines Unternehmens verwendet werden. Alle Elemente oder Teilelemente, die zur Implementierung der Sicherheitsregeln eingesetzt werden können, sind sicherheitsrelevant und Bestandteil der TCB. Bei der TCB handelt es sich um ein Objekt, das durch die Sicherheitsperipherie begrenzt wird. Die Mechanismen, die zur praktischen Umsetzung der Sicherheitsregeln eingesetzt werden, dürfen nicht umgangen werden können und müssen verhindern, dass Programme Zugriff auf Systemprivilegien erlangen können, für die sie nicht berechnigt sind.

H

Hierarchie

Die Organisation von Zertifikatsausstellern (CAs) innerhalb einer Trust-Kette. Diese beginnt mit einem selbst unterzeichnenden CA oder übergeordneten Root-CA, der sich an der höchsten Position befindet, und endet mit dem CA, der Zertifikate für Endbenutzer ausstellt.

Höchster CA

Der CA, der innerhalb der PKI-CA-Hierarchie die höchste Position einnimmt.

HTML

Hypertext Markup Language.

HTTP

Hypertext Transaction Protocol.

HTTP-Server

Ein Server, der die Web-gestützte Kommunikation mit Browsern und anderen Programmen im Netz steuert.

Hypertext

Textsegmente, die einzelne oder mehrere Wörter umfassen oder Bilder enthalten, auf die der Leser mit der Maus klicken kann, um ein anderes Dokument aufzurufen und anzuzeigen. Diese Textsegmente werden als Hyperlinks bezeichnet. Ruft der Leser diese anderen Dokumente auf, stellt er zu diesen eine Hyperlink-Verbindung her.

Hypertext Markup Language (HTML)

Eine Formatierungssprache für das Codieren von Web-Seiten. HTML basiert auf SGML (Standard Generalized Markup Language).

Hypertext Transaction Protocol (HTTP)

Ein Client/Server-Protokoll für das Internet, mit dem Hypertext-Dateien im Web übertragen werden.

ICL

Issued Certificate List - Liste der ausgestellten Zertifikate.

Identitätsnachweis

Vertrauliche Informationen, die verwendet werden, um beim Austausch von Daten während der Authentifizierung die eigene Identität zu belegen. In Network Computing-Umgebungen ist die am häufigsten verwendete Form des Identitätsnachweises ein Zertifikat, das von einem CA erstellt und unterzeichnet wurde.

IniEditor

Bei Tivoli PKI ein Tool, mit dem Konfigurationsdateien editiert werden können.

Integrität

Ein System schützt seine Datenintegrität, wenn es die Änderung dieser Daten durch nicht berechtigte Personen verhindert. (Im Gegensatz hierzu versteht man unter dem Schutz der Vertraulichkeit von Daten, wenn verhindert wird, dass diese unberechtigten Personen zugänglich gemacht werden.)

Integritätsprüfung

Die Prüfung der Protokolleinträge, die für Transaktionen mit externen Komponenten aufgezeichnet wurden.

International Standards Organization (ISO)

Eine internationale Organisation, die sich mit der Entwicklung und Veröffentlichung von Standards befasst.

International Telecommunication Union (ITU)

Eine internationale Organisation, in der Verwaltungs- und private Industriebereiche globale Datenfernübertragungsnetze und -services koordinieren. Bei der Veröffentlichung von Informationen zur Datenfernübertragungstechnologie sowie den entsprechenden Regelwerken und Standards nimmt sie eine führende Position ein.

Interne Struktur

Siehe Schema.

Internet

Ein weltweiter Verbund von Netzen, die die elektronische Verbindung zwischen Computern und die Kommunikation zwischen den Computern über Softwareeinrichtungen wie elektronische Post (E-Mail) oder Web-Browser ermöglichen. So sind beispielsweise die meisten Universitäten in ein Netz eingebunden, das seinerseits eine Verbindung zu anderen ähnlichen Netzen hat, die zusammen das Internet bilden.

Internet Engineering Task Force (IETF)

Eine Gruppe, die sich schwerpunktmäßig mit dem Entwickeln und Definieren von Protokollen für das Internet befasst. Sie repräsentiert eine internationale Gruppe von Netzdesignern, -bedienern, -herstellern und -forschern. Die Aufgabe der IETF ist die Entwicklung der Internet-Architektur sowie die Gewährleistung der reibungslosen Verwendung des Internets.

Intranet

Ein Netz innerhalb eines Unternehmens, das sich im Allgemeinen hinter Firewalls befindet. Es basiert auf dem Internet und setzt eine ähnliche Technologie ein. Vom technischen Standpunkt aus ist ein Intranet eine Erweiterung des Internets. Zu den in beiden Netzen benutzten Komponenten gehören z. B. HTML und HTTP.

IPSec

Ein von der IETF entwickelter IPS-Standard (IPS = Internet Protocol Security). IPSec ist ein Protokoll der Vermittlungsschicht, das entwickelt wurde, um Services für die Gewährleistung der Sicherheit bei der Verschlüsselung zur Verfügung zu stellen, die kombinierte Funktionen zur Authentifizierung, Sicherung der Integrität, Zugriffssteuerung und Wahrung der Vertraulichkeit flexibel unterstützen. Aufgrund seiner leistungsfähigen Funktionen bei der Authentifizierung wurde dieser Standard von vielen Lieferanten von VPN-Produkten als Protokoll zum Aufbau sicherer Punkt-zu-Punkt-Verbindungen im Internet übernommen.

ISO

International Standards Organization.

ITU

International Telecommunication Union.

J

Java

Von Sun Microsystems, Incorporated, entwickelte plattformunabhängige Computertechnologien, die für den Netzbetrieb optimiert sind. Die Java-Umgebung besteht aus dem Java-Betriebssystem (Java-OS), den virtuellen Maschinen für verschiedene Plattformen, der objektorientierten Java-Programmiersprache und einer Reihe von Klassenbibliotheken.

Java-Anwendung

Ein eigenständiges Programm, das in der Programmiersprache Java geschrieben ist. Es wird außerhalb eines Web-Browsers ausgeführt.

Java-Applet

Siehe Applet. Gegensatz zu Java-Anwendung.

Java-Klasse

Eine Einheit mit Java-Programmcode.

Java-Sprache

Eine von Sun Microsystems entwickelte Programmiersprache, die speziell für die Verwendung in Applet- und Agent-Anwendungen konzipiert wurde.

Java Virtual Machine (JVM)

Der Teil der Java-Laufzeitumgebung, der zum Interpretieren von Bytecodes eingesetzt wird.

K

KeyStore (Schlüsselspeicher)

Eine DL zum Speichern von Identitätsnachweisen für Tivoli PKI-Komponenten, z. B. Schlüssel und Zertifikate, in einem verschlüsselten Format.

Klartext

Nicht verschlüsselte Daten. *Synonym zu unverschlüsselter Text.*

Klasse

Beim objektorientierten Entwurf bzw. bei der objektorientierten Programmierung eine Gruppe von Objekten, die über eine gemeinsame Definition verfügen und aus diesem Grund mit denselben Merkmalen, Verarbeitungsoperationen und Funktionsweisen arbeiten.

Kryptographie

Bei der Sicherung von Computern die Prinzipien, Verfahren und Methoden zur Verschlüsselung von unverschlüsseltem und zur Entschlüsselung von verschlüsseltem Text.

L**LDAP**

Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)

Ein Protokoll, mit dem auf das Directory zugegriffen werden kann.

Liste der ausgestellten Zertifikate (ICL)

Eine vollständige Liste der ausgestellten Zertifikate sowie deren aktueller Status. Die Zertifikate sind anhand der Seriennummer und des Status indexiert. Diese Liste wird vom CA verwaltet und in der CA-Datenbank gespeichert.

M**MAC**

Message Authentication Code - Nachrichtenauthentifizierungscode.

MD4

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Ihre Geschwindigkeit übersteigt die von MD2 um ein Mehrfaches.

MD5

Eine unidirektionale Nachrichtenauszugs-Hash-Funktion, die von Ron Rivest entwickelt wurde. Sie stellt eine verbesserte Version von MD4 dar. MD5 verarbeitet Eingabetext in 512-Bit-Blöcken, die in 16 32-Bit-Unterblöcke aufgeteilt werden. Die Ausgabe des Algorithmus ist eine Gruppe von vier 32-Bit-Blöcken, die verkettet werden und so einen 128-Bit-Hash-Wert bilden. Diese Funktion wird ebenfalls zusammen mit MD2 in dem PEM-Protokollen verwendet.

MD2

Eine Nachrichtenauszugs-Hash-Funktion auf 128-Bit-Basis, die von Ron Rivest entwickelt wurde. Sie wird zusammen mit MD5 in den PEM-Protokollen verwendet.

Modulus

In dem auf öffentlichen Schlüsseln basierenden RSA-Verschlüsselungssystem das Produkt (n) aus zwei hohen Primzahlen: p und q . Die optimale Größe für einen RSA-Modulus hängt von den individuellen Sicherheitsanforderungen ab. Je größer der Modulus, desto höher die Sicherheit. Die momentan von den RSA Laboratories empfohlenen Schlüsselgrößen hängen vom geplanten Einsatz des Schlüssels ab. Hierbei werden 768 Bit für Schlüssel zum persönlichen Gebrauch, 1024 Bit für den Unternehmensbereich und 2048 Bit für extrem wertvolle Schlüssel wie z. B. CA-Schlüsselpaare angegeben. Ein 768-Bit-Schlüssel wird voraussichtlich bis mindestens zum Jahr 2004 sicher sein.

Multipurpose Internet Mail Extensions (MIME)

Eine frei verfügbare Gruppe von Spezifikationen, die den Austausch von Text in Sprachen mit unterschiedlichen Zeichensätzen ermöglicht. Diese Spezifikationen unterstützen auch den Austausch von Multimedia-E-Mail zwischen unterschiedlichen Computersystemen, die Internet-Mail-Standards verwenden. So können E-Mail-Nachrichten beispielsweise andere Zeichensätze als den US-ASCII-Satz sowie erweiterten Text, Bilder oder Tondaten enthalten.

N

Nachrichtenauszug

Eine irreversible Funktion, bei der auf der Basis einer Nachricht beliebiger Länge eine Datenmenge mit fester Länge generiert wird. Bei MD5 handelt es sich z. B. um einen Nachrichtenauszugsalgorithmus.

Nachrichtenauthentifizierungscode (MAC)

Ein geheimer Schlüssel, der von Sender und Empfänger gemeinsam benutzt wird. Der Sender authentifiziert sich und der Empfänger prüft die hierbei zur Verfügung gestellten Daten. Bei Tivoli PKI werden MAC-Schlüssel für CA- und Prüfkomponten in den KeyStores gespeichert.

National Security Agency (NSA)

Die offizielle Sicherheitsbehörde der US-Regierung.

NIST

National Institute of Standards and Technology, früher NBS (National Bureau of Standards). Aufgabe dieses Instituts ist die Unterstützung offener Standards und der Interoperabilität in den verschiedenen Bereichen der Computerbranche.

NLS

National Language Support - Unterstützung in der Landessprache.

NSA

National Security Agency.

O

Objekt

Beim objektorientierten Design oder bei der objektorientierten Programmierung eine abstrakte Entität, die zur Abgrenzung bestimmter Daten und der zugehörigen Operationen dient. *Siehe auch* Klasse.

Objektart

Die Art von Objekt, die im Directory gespeichert werden kann. Beispiele sind eine Firma, ein Konferenzraum, eine Einheit, eine Person, ein Programm oder ein Prozess.

Objekt-ID (OID)

Ein von einer Verwaltungsfunktion zugeordneter Datenwert, der den in ASN.1 definierten Typ aufweist.

ODBC

Open Database Connectivity.

Öffentlicher Schlüssel

In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel anderen Benutzern zur Verfügung. Er ermöglicht diesen Benutzern die Weiterleitung einer Transaktion an den Eigner des Schlüssels sowie die Prüfung einer digitalen Unterschrift. Mit einem öffentlichen Schlüssel verschlüsselte Daten können nur mit dem entsprechenden privaten Schlüssel entschlüsselt werden. *Gegensatz zu* Privater Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.

Open Database Connectivity (ODBC)

Ein Standard für den Zugriff auf unterschiedliche Datenbanksysteme.

Open Systems Interconnect (OSI)

Der Name der von ISO genehmigten Computernetzstandards.

OSI

Open Systems Interconnect.

P

PC-Karte

Eine mit einer Smart-Card vergleichbare Einheit, die auch als PCMCIA-Karte bezeichnet wird. Sie ist etwas größer als eine Smart-Card und verfügt im Allgemeinen über eine höhere Kapazität.

-
- PEM**
Privacy-Enhanced Mail.
- PKCS**
Public Key Cryptography Standards.
- PKCS #1**
Siehe Public Key Cryptography Standards.
- PKCS #7**
Siehe Public Key Cryptography Standards.
- PKCS #10**
Siehe Public Key Cryptography Standards.
- PKCS #11**
Siehe Public Key Cryptography Standards.
- PKCS #12**
Siehe Public Key Cryptography Standards.
- PKI**
Public Key Infrastructure.
- PKIX**
PKI auf X.509v3-Basis.
- PKIX Certificate Management Protocol (PKIX CMP)**
Ein Protokoll, das Verbindungen mit PKIX-kompatiblen Anwendungen ermöglicht. PKIX CMP verwendet als primäres Transportverfahren TCP/IP, es ist jedoch eine Abstraktionsebene oberhalb der Sockets-Schicht vorhanden. Dies ermöglicht die Unterstützung für zusätzliche Datenübertragungsoperationen mit Sendeaufrufen (Polling).
- PKIX CMP**
PKIX Certificate Management Protocol.
- PKIX-Empfangseinheit**
Der öffentliche HTTP-Server, der von einer bestimmten Registrierungsdomäne verwendet wird, um Anforderungen der Client-Anwendung von Tivoli PKI zu empfangen.
- Privacy-Enhanced Mail (PEM)**
Der vom Internet Architect Board (IAB) genehmigte Internet-Standard für die verbesserte Wahrung der Vertraulichkeit, der die sichere Übertragung elektronischer Post (E-Mail) über das Internet ermöglicht. Die PEM-Protokolle regeln Verschlüsselung, Authentifizierung, Nachrichtenintegrität und Schlüsselverwaltung.
- Privater Schlüssel**
In einem Paar aus einem öffentlichen und einem privaten Schlüssel steht dieser Schlüssel nur für seinen Eigner zur Verfügung. Er ermöglicht dem Eigner das Empfangen einer privaten Transaktion oder eine digitale Unterschrift. Die mit einem privaten Schlüssel unterzeichneten Daten können nur mit dem entsprechenden öffentlichen Schlüssel geprüft werden. *Gegensatz zu* öffentlicher Schlüssel. *Siehe auch* Schlüsselpaar aus öffentlichem und privatem Schlüssel.
- Protokoll**
Eine vereinbarte Konvention für die Kommunikation zwischen Computern.
- Protokollierungssystem**
Bei Tivoli PKI ein Subsystem, das die Unterstützungsfunktionen zum Protokollieren von sicherheitsrelevanten Aktionen bereitstellt. Es entspricht den Empfehlungen, die im X9.57-Standard unter *Public Key Cryptography for the Financial Services Industry* definiert wurden.
- Proxy-Server**
Eine Einheit, die zwischen einem Computer, der eine Zugriffsanforderung absetzt (Computer A) und einem Computer, auf den zugegriffen werden soll (Computer B), implementiert ist. Wenn ein Endbenutzer eine Anforderung für eine Ressource über Computer A absetzt, wird diese an den Proxy-Server geleitet. Dieser sendet die Anforderung

ung an Computer B, erhält von diesem die Antwort und leitet diese an den Endbenutzer weiter. Mit Hilfe eines Proxy-Servers kann über einen Computer, der sich innerhalb einer Firewall befindet, auf das World Wide Web zugegriffen werden.

Prüf-Client

Jeder Client im System, der Prüfereignisse an den Tivoli PKI-Prüf-Server sendet. Bevor ein Prüf-Client ein Ereignis an den Prüf-Server sendet, stellt er eine Verbindung zu diesem her. Nach der Herstellung der Verbindung verwendet der Client die Client-Bibliothek des Prüfsubsystems, um Ereignisse an den Prüf-Server zu übertragen.

Prüfprotokoll

Daten in Form eines logischen Pfades, die eine Folge von Ereignissen verbinden. Mit dem Prüfprotokoll können Transaktionen oder der bisherige Verlauf einer bestimmten Aktivität verfolgt werden.

Prüfprotokoll

Bei Tivoli PKI eine Tabelle in einer Datenbank, in der für jedes Prüfereignis ein Datensatz gespeichert wird.

Prüf-Server

Ein Tivoli PKI-Server, der zum Empfangen von Prüfereignissen von Prüf-Clients und zum Aufzeichnen dieser Ereignis in einem Prüfprotokoll dient.

Prüfzeichenfolge

Eine Zeichenfolge, die von einem Server oder einer Anwendung gesendet wird und zum Anfordern der Benutzerberechtigung dient. Der Benutzer, der zur Authentifizierung aufgefordert wird, unterzeichnet die Prüfzeichenfolge mit einem privaten Schlüssel. Der öffentliche Schlüssel des Benutzers sowie die unterzeichnete Prüfzeichenfolge werden zurück an den Server oder die Anwendung gesendet, der bzw. die die Authentifizierung anforderte. Der Server versucht anschließend, die unterzeichnete Prüfzeichenfolge mit Hilfe des öffentlichen Schlüssels des Benutzers zu entschlüsseln. Wenn die entschlüsselte Prüfzeichenfolge mit der ursprünglich gesendeten Prüfzeichenfolge übereinstimmt, gilt der Benutzer als authentifiziert.

Public Key Cryptography Standards (PKCS)

Informelle, herstellerübergreifende Standards, die im Jahr 1991 von den RSA Laboratories in Zusammenarbeit mit Repräsentanten verschiedener Computerhersteller entwickelt wurden. Diese Standards umfassen die RSA-Verschlüsselung, die Diffie-Hellman-Vereinbarung, die kennwortbasierte Verschlüsselung sowie die Syntax für erweiterte Zertifikate, verschlüsselte Nachrichten, Daten zu privaten Schlüsseln und für die Zertifizierung.

- PKCS #1 beschreibt ein Verfahren zum Verschlüsseln von Daten mit Hilfe des RSA-Verschlüsselungssystems auf der Basis öffentlicher Schlüssel. Er dient zur Erstellung digitaler Unterschriften und Briefumschläge.
- PKCS #7 definiert ein allgemeines Format für verschlüsselte Nachrichten.
- PKCS #10 definiert eine Standardsyntax für Zertifizierungsanforderungen.
- PKCS #11 definiert eine Programmierschnittstelle für Verschlüsselungseinheiten, z. B. Smart-Cards, die unabhängig vom verwendeten technologischen Konzept ist.
- PKCS #12 definiert ein portierbares Format zum Speichern oder Transportieren der privaten Schlüssel, Zertifikate und sonstiger geheimer Daten etc. eines Benutzers.

Public Key Infrastructure (PKI)

Ein Standard für Sicherheitssoftware, der auf der Verschlüsselung mit Hilfe öffentlicher Schlüssel basiert. Bei PKI handelt es sich um ein System digitaler Zertifikate, Zertifikatsaussteller, Registrierungsstellen, Zertifikatsverwaltungsservices und verteilter Verzeichnisservices. Er dient zum Prüfen der Identität und Berechtigung aller Parteien, die an Transaktionen beteiligt sind, die über das Internet ausgeführt werden. Diese Transaktionen umfassen möglicherweise Operationen, zu deren Ausführung eine Identitätsprüfung erforderlich ist. Sie dienen z. B. zur Bestätigung des Ursprungs von Senderechanforderungen, E-Mail-Nachrichten oder Finanztransaktionen.

PKI stellt öffentliche Chiffrierschlüssel und Benutzerzertifikate für die Authentifizierung durch eine berechtigte Einzelperson oder ein berechtigtes Unternehmen zur Verfügung. Er stellt Online-Verzeichnisse bereit, die die öffentlichen Chiffrierschlüssel und Zertifikate enthalten, die zur Überprüfung der digitalen Zertifikate, Identitätsnachweise sowie der digitalen Unterschriften verwendet werden.

PKI stellt außerdem Funktionen zur schnellen und effizienten Antwort auf Prüfabfragen und Anforderungen für öffentliche Chiffrierschlüssel bereit. Der Standard dient darüber hinaus zur Identifizierung potenzieller Sicherheitslücken im System und zur Verwaltung von Ressourcen zur Bearbeitung von Sicherheitsverletzungen. PKI bietet außerdem einen digitalen Zeitmarkenservice für wichtige Unternehmenstransaktionen.

R

RA

Registration Authority - Registrierungsstelle.

RA Desktop

Ein Java-Applet, das den RAs eine Grafikschnittstelle für die Verarbeitung von Anforderungen für Identitätsnachweise und zur Verwaltung dieser Nachweise während ihrer Gültigkeitsdauer zur Verfügung stellt.

RA-Server

Der Server für die RA-Komponente von Tivoli PKI.

RC2

Eine variable Schlüsselgrößen-Block-Cipher, die von Ron Rivest für RSA Data Security entwickelt wurde. *RC* steht für *Ron's Code* oder *Rivest's Cipher*. Sie arbeitet schneller als DES und löst diese Block-Cipher ab. Durch die Verwendung geeigneter Schlüsselgrößen kann sie in Bezug auf eine ausgedehnte Schlüsselsuche flexibler als DES gestaltet werden. Sie verfügt über eine Blockgröße von 64 Bit und arbeitet auf Softwareebene zwei- bis dreimal schneller als DES. RC2 kann in denselben Modi eingesetzt werden wie DES. Durch eine Vereinbarung zwischen SPA (Software Publishers Association) und der US-Regierung nimmt RC2 einen speziellen Status ein. Hierdurch ist das Genehmigungsverfahren für den Export einfacher und schneller, als dies bei anderen Verschlüsselungsprodukten der Fall ist. Um die Voraussetzungen für eine rasche Exportgenehmigung zu erfüllen, muss ein Produkt mit einigen Ausnahmen die RC2-Schlüsselgröße auf 40 Bit beschränken. Eine zusätzliche Zeichenfolge kann verwendet werden, um Nichtberechtigte abzuwehren, die versuchen, eine umfangreiche Tabelle möglicher Verschlüsselungsvarianten vorzuberechnen.

Regel-Exit

In einer Registrierungsfunktion ein auf Unternehmensebene definiertes Programm, das von der Registrierungsanwendung aufgerufen wird. Die Regeln eines Regel-Exits implementieren die Unternehmens- und Sicherheitsbenutzervorgaben eines Unternehmens für den Registrierungsprozess.

Registrierter Name (DN)

Der eindeutige Name eines im Directory gespeicherten Dateneintrags. Der DN dient zur eindeutigen Identifizierung der Position eines Eintrags in der hierarchischen Struktur des Directory.

Registrierung

Bei Tivoli PKI das Abrufen von Identitätsnachweisen für die Verwendung über das Internet. Bei der Registrierung werden Zertifikate angefordert, erneuert und widerrufen.

Registrierungsattribut

Eine Registrierungsvariable, die in einem Registrierungsformular enthalten ist. Ihr Wert gibt die Informationen wider, die während der Registrierung erfasst werden. Der Wert des Registrierungsattributs bleibt während der gesamten Gültigkeitsdauer des Identitätsnachweises gleich.

Registrator

Ein Benutzer, der für den Zugriff auf RA Desktop sowie zur Verwaltung und Anforderung von Zertifikaten berechtigt ist.

Registrierungsstelle (RA)

Die Software, die zur Verwaltung digitaler Zertifikate verwendet wird und sicherstellt, dass die Unternehmensregeln vom ersten Empfang einer Registrierungsanforderung bis zum Zertifikatswiderruf angewendet werden.

Registrierungsdatenbank

Diese Datenbank enthält Informationen zu Zertifikatsanforderungen und ausgestellten Zertifikaten. In der Datenbank werden Registrierungsdaten gespeichert und alle Änderungen aufgezeichnet, die während der Gültigkeitsdauer an einem Zertifikat vorgenommen werden. Die Datenbank kann durch RA-Prozesse und Regel-Exits oder durch den Registrator aktualisiert werden.

Registrierungsdomäne

Eine Gruppe von Ressourcen, Regeln und Konfigurationsoptionen, die sich auf bestimmte Registrierungsprozesse für Zertifikate beziehen. Der Domänenname stellt einen untergeordneten Wert zur URL-Adresse dar, die zur Ausführung der Registrierungsfunktion eingesetzt wird.

Registrierungsfunktion

Ein Tivoli PKI-Anwendungsgerüst, das spezielle Verfahren zur Registrierung von Entitäten (z. B. Browser, Router, E-Mail-Einheiten und sichere Client-Anwendungen) und zur Verwaltung von Zertifikaten während ihrer Gültigkeitsdauer bereitstellt.

Registrierungsprozess

Bei Tivoli PKI die Schritte, die zur Überprüfung eines Benutzers ausgeführt werden. Durch den Registrierungsprozess werden Benutzer sowie deren öffentliche Schlüssel zertifiziert, um sie zur Teilnahme an den gewünschten Transaktionen zu berechtigen. Er kann lokal oder Web-gestützt, automatisch oder von einer tatsächlich mit Personen besetzten Registrierungsstelle ausgeführt werden.

Registrierungsvariable

Siehe Registrierungsattribut.

RSA

Ein auf öffentlichen Schlüsseln basierender Verschlüsselungsalgorithmus, der nach seinen Erfindern (Rivest, Shamir und Adelman) benannt wurde. Er wird zur Verschlüsselung und für digitale Unterschriften verwendet.

S

Schema

Beim Directory die interne Struktur, die zur Definition der Beziehungen zwischen den verschiedenen Objektarten verwendet wird.

Schlüssel

Bei der Verschlüsselung ein Wert, der zum Ver- und Entschlüsseln von Informationen verwendet wird.

Schlüsselpaar

Zusammengehörende Schlüssel, die bei der asymmetrischen Verschlüsselung eingesetzt werden. Ein Schlüssel wird zur Verschlüsselung, der andere zur Entschlüsselung verwendet.

Schlüsselpaar aus öffentlichem und privatem Schlüssel

Ein Schlüsselpaar aus öffentlichem und privatem Schlüssel stellt ein grundlegendes Element der Verschlüsselung auf der Basis von Schlüsselpaaren dar. (Diese Form der Verschlüsselung wurde im Jahr 1976 von Whitfield Diffie und Martin Hellman eingeführt, um Probleme bei der Schlüsselverwaltung zu lösen.) Nach diesem Konzept erhält jeder Benutzer ein Schlüsselpaar, bei dem einer als öffentlicher und einer als privater Schlüssel bezeichnet wird. Der öffentliche Schlüssel ist hierbei allgemein bekannt, der private Schlüssel wird hingegen geheim gehalten. Sender und Empfänger müssen geheime Daten nicht gemeinsam benutzen. Alle Kommunikationsoperationen werden lediglich auf der Basis öffentlicher Schlüssel ausgeführt. Die privaten Schlüssel werden niemals übertragen oder gemeinsam verwendet. Auf diese Weise ist es nicht mehr notwendig, sich auf die Sicherheit eines Übertragungskanals gegenüber Manipulationen zu verlassen. Die einzige Anforderung ist, dass öffentliche Schlüssel den entsprechenden Benutzern in einer gesicherten (authentifizierten) Weise (z. B. in einem gesicherten Verzeichnis) zugeordnet werden. Jeder Benutzer kann nun mit Hilfe dieser öffentlichen Daten eine vertrauliche Nachricht senden. Diese Nachricht kann nur mit einem privaten Schlüssel entschlüsselt werden, auf den allein der gewünschte Empfänger zugreifen kann. Darüber hinaus kann die Verschlüsselung auf der Basis von Schlüsselpaaren nicht nur zur Gewährleistung der Vertraulichkeit (Verschlüsselung), sondern auch für die Authentifizierung (digitale Unterschriften) eingesetzt werden.

Schlüsselsicherung und -wiederherstellung

Diese Funktion von Tivoli PKI ermöglicht das Sichern und Wiederherstellen von Endentitätszertifikaten und der zugehörigen, von Tivoli PKI zertifizierten öffentlichen und privaten Schlüssel. Die Zertifikate und Schlüssel werden in einer PKCS #12-Datei gespeichert. Diese Datei ist kennwortgeschützt. Das Kennwort wird beim Sichern des Zertifikats und der Schlüssel gesetzt.

Secure Electronic Transaction (SET)

Ein Branchenstandard für die Durchführung sicherer Kredit- oder Kundenkartenzahlungen über nicht gesicherte Netze. Der Standard formuliert Definitionen für die Authentifizierung von Kartenhaltern, Händlern sowie der Banken, durch die die Karten ausgestellt werden, da er die Ausstellung von Zertifikaten anfordert.

Secure Sockets Layer (SSL)

Ein IETF-Standardübertragungsprotokoll mit integrierten Sicherheitsservices, die für den Endbenutzer möglichst transparent sind. Es stellt einen digitalen, sicheren Kommunikationskanal zur Verfügung.

Ein SSL-fähiger Server empfängt SSL-Verbindungsanforderungen im Allgemeinen an einem anderen Anschluss (Port) als normale HTTP-Anforderungen. SSL erstellt eine Sitzung, in der die Austauschsignale zum Herstellen der Kommunikation zwischen zwei Modems nur einmal gesendet werden müssen. Anschließend wird die Kommunikation verschlüsselt und die Nachrichtenintegrität wird solange überprüft, bis die SSL-Sitzung abgelaufen ist.

Server

(1) In einem Netz eine Datenstation, die anderen Stationen Funktionen zur Verfügung stellt, wie beispielsweise ein Datei-Server. (2) In TCP/IP ein System in einem Netz, das die Anforderungen eines Systems an einem anderen Standort verarbeitet. Dieses Konzept wird als Client/Server-Modell bezeichnet.

Server-Zertifikat

Ein digitales Zertifikat, das von einem CA ausgegeben wird und es einem Web-Server ermöglicht, SSL-gestützte Transaktionen auszuführen. Wenn ein Browser über das SSL-Protokoll eine Verbindung zum Server herstellt, sendet der Server seinen öffentlichen Schlüssel an den Browser. Hierdurch kann die Identität des Servers authentifiziert werden und es können verschlüsselte Daten an den Server gesendet werden. *Siehe auch* CA-Zertifikat, Digitales Zertifikat *und* Browserzertifikat.

Servlet

Ein Server-Programm, das zusätzliche Funktionen für Server zur Verfügung stellt, die Java unterstützen.

SET

Secure Electronic Transaction.

SGML

Standard Generalized Markup Language.

SHA-1 (Secure Hash Algorithm)

Ein von NIST und NSA entwickelter Algorithmus, der beim DSS (Digital Signature Standard) verwendet wird. Der Standard wird als Secure Hash Standard bezeichnet; SHA ist der Algorithmus, der von diesem Standard verwendet wird. Er generiert einen 160-Bit-Hash-Code.

Sicherheitsdomäne

Eine Gruppe (z. B. Unternehmen, Arbeitsgruppe, Projektteam), deren Zertifikate vom gleichen CA zertifiziert wurden. Benutzer, die über ein von einem CA unterzeichnetes Zertifikat verfügen, können der Identität eines anderen Benutzers vertrauen, der ein Zertifikat besitzt, das vom selben CA unterzeichnet worden ist.

Sicherungsmodell

Eine Organisationskonvention, die regelt, wie Zertifikatsaussteller (CAs) andere Zertifikatsaussteller zertifizieren können.

Simple Mail Transfer Protocol (SMTP)

Ein Protokoll, mit dem elektronische Post über das Internet übertragen wird.

Site-Zertifikat

Dieser Zertifikatstyp ist mit einem CA-Zertifikat vergleichbar, gilt jedoch nur für eine bestimmte Website. *Siehe auch* CA-Zertifikat.

Smart-Card

Eine Hardwarekomponente, normalerweise in der Größe einer Kreditkarte, auf der die digitalen Schlüssel eines Benutzers gespeichert werden können. Eine Smart-Card kann kennwortgeschützt werden.

S/MIME

Ein Standard, der das Unterzeichnen und Verschlüsseln von elektronischer Post (E-Mail) unterstützt, die über das Internet übertragen wird. *Siehe* MIME.

SMTP

Simple Mail Transfer Protocol.

SSL

Secure Sockets Layer.

Standard Generalized Markup Language (SGML)

Ein Standard zur Beschreibung von Formatierungssprachen. HTML basiert auf SGML.

Symmetrischer Schlüssel

Ein Schlüssel, der sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden kann. *Siehe auch* Symmetrische Verschlüsselung.

Symmetrische Verschlüsselung

Eine Form der Verschlüsselung, bei der sowohl für die Ver- als auch für die Entschlüsselung derselbe Schlüssel verwendet wird. Die Sicherheit dieses Verfahrens basiert auf dem Schlüssel. Wird dieser öffentlich bekannt gegeben, können die mit ihm bearbeiteten Nachrichten von jedem Benutzer ver- und entschlüsselt werden. Der Inhalt der übertragenen Daten kann nur dann geheim gehalten werden, wenn der Schlüssel nur den jeweils berechtigten Personen bekannt ist. *Gegensatz zu* Asymmetrische Verschlüsselung.

T**TCP/IP**

Transmission Control Protocol/Internet Protocol.

TP

Trust Policy = Sicherungsregel.

Transaktions-ID

Eine Kennung, die die RA als Antwort auf eine Anforderung für eine Vorabregistrierung zur Verfügung stellt. Mit dieser ID kann ein Benutzer, der die Client-Anwendung von Tivoli PKI ausführt, ein vorab genehmigtes Zertifikat erhalten.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Eine Gruppe von Übertragungsprotokollen, die Peer-zu-Peer-Konnektivitätsfunktionen für lokale Netze (LANs) und Weitverkehrsnetze (WANs) unterstützen.

Triple DES

Ein symmetrischer Algorithmus, bei dem der unverschlüsselte Text dreimal verschlüsselt wird. Obwohl für diese Mehrfachverschlüsselung zahlreiche Methoden existieren, stellt die Triple DES-Verschlüsselung, die auf drei verschiedenen Schlüsseln basiert, das sicherste dieser Verfahren dar.

Tivoli PKI

Eine integrierte IBM Sicherheitslösung, die die Ausstellung, Erneuerung und den Widerruf digitaler Zertifikate unterstützt. Diese Zertifikate können für eine breite Palette von Internet-Anwendungen eingesetzt werden und bieten eine Möglichkeit zur Authentifizierung von Benutzern und zur Gewährleistung einer gesicherten Kommunikation.

Trust-Kette

Eine Gruppe von Zertifikaten, die aus der gesicherten Hierarchie vom Benutzerzertifikat bis zum Root- oder selbstunterzeichneten Zertifikat besteht.

Tunnel

In der VPN-Technologie eine virtuelle Punkt-zu-Punkt-Verbindung, die auf Anfrage über das Internet hergestellt wird. Während der Verbindung können ferne Benutzer den Tunnel verwenden, um sichere, verschlüsselte und gekapselte Informationen mit Servern im privaten Netz eines Unternehmens auszutauschen.

U**Unbestreitbarkeit**

Die Verwendung eines digitalen, privaten Schlüssels, um zu verhindern, dass der Unterzeichner eines Dokuments dessen Unterzeichnung leugnet.

Unicode

Ein 16-Bit-Zeichensatz, der in ISO 10646 definiert ist. Der Unicodestandard für die Verschlüsselung von Zeichen ist ein internationaler Zeichencode für die Informationsverarbeitung. Er umfasst die grundlegenden, weltweit verwendeten Prozeduren und bildet die Basis für die Internationalisierung und Lokalisierung von Software. Der gesamte Quellencode in der Java-Programmierungsumgebung wird in Unicode geschrieben.

Unternehmensprozessobjekte

Eine Codegruppe, die zur Ausführung einer bestimmten Registrierungsoperation, z. B. zum Prüfen des Registrierungsstatus oder zur Bestätigung des Sendens eines öffentlichen Schlüssels, verwendet wird.

Unternehmensprozessschablone

Eine Gruppe von Unternehmensprozessobjekten, die in einer bestimmten Reihenfolge ausgeführt werden.

Unterstützung in der Landessprache (NLS)

Unterstützung für unterschiedliche länderspezifische Angaben in einem Produkt. Hierzu gehören die Sprache, die Währung, das Datums- und Zeitformat und die Darstellung von Zahlen.

Unterzeichnen

Die Verwendung eines digitalen privaten Schlüssels zum Generieren einer Unterschrift. Diese Unterschrift dient dazu, zu beweisen, dass ein bestimmter Benutzer für die von ihm unterzeichnete Nachricht verantwortlich ist und diese akzeptiert.

Unterzeichnen/Prüfen

Als Unterzeichnen wird die Verwendung eines privaten Schlüssels zum Generieren einer Unterschrift bezeichnet. Unter Prüfen versteht man die Verwendung des entsprechenden öffentlichen Schlüssels zur Verifizierung dieser Unterschrift.

Unverschlüsselter Text

Nicht verschlüsselte Daten. *Synonym zu Klartext.*

URL

Uniform Resource Locator - URL-Adresse.

URL-Adresse

Ein Schema für die Adressierung von Ressourcen im Internet. Die URL-Adresse gibt das verwendete Protokoll sowie den Host-Namen und die IP-Adresse an. Außerdem enthält er Angaben zur Anschlussnummer, zum Pfad sowie weitere Ressourcendetails, die erforderlich sind, um über eine bestimmte Maschine auf eine Ressource zuzugreifen.

UTF-8

Ein Umsetzungsformat. Es ermöglicht Informationsverarbeitungssystemen, die nur die Verarbeitung von 8-Bit-Zeichensätzen unterstützen, die Umsetzung von 16-Bit-Unicode in ein 8-Bit-Äquivalent und umgekehrt, ohne dass hierbei Informationen verloren gehen.

V**Verkettungsprüfung**

Die Gültigkeitsprüfung aller CA-Unterschriften in der Trust-Hierarchie, über die ein bestimmtes Zertifikat ausgestellt wurde. Wenn z. B. das Unterschriftszertifikat eines CA über einen anderen CA ausgestellt wurde, werden bei der Gültigkeitsprüfung des vom Benutzer vorgelegten Zertifikats beide Unterschriften geprüft.

Verschlüsseln

Das Umordnen von Informationen, so dass nur Personen, die über den richtigen Entschlüsselungscode verfügen, die ursprünglichen Informationen durch Entschlüsselung abrufen können.

Verschlüsselt

Die Eigenschaft von Daten, die nach einem bestimmten System umgesetzt wurden, um deren Bedeutung unkenntlich zu machen.

Verschlüsselung/Entschlüsselung

Die Verwendung des öffentlichen Schlüssels des gewünschten Empfängers zum Verschlüsseln von Daten für diese Person. Der Empfänger verwendet anschließend den privaten Schlüssel seines Schlüsselpaares, um die Daten zu entschlüsseln.

Vertrauensdomäne

Eine Gruppe von Entitäten, deren Zertifikate vom gleichen CA zertifiziert wurden.

Vertraulichkeit

Der Schutz von Daten gegen den Zugriff nicht berechtigter Personen.

Vertraulichkeit

Die Wahrung der Geheimhaltung bestimmter Informationen gegenüber nicht berechtigten Personen.

Virtual Private Network (VPN)

Ein privates Datennetz, das ferne Verbindungen nicht über Telefonleitungen, sondern über das Internet herstellt. Da der Zugriff der Benutzer auf die Netzressourcen eines Unternehmens nicht über eine Telefongesellschaft, sondern über einen Internet Service Provider (ISP) erfolgt, können diese durch den Einsatz von VPN deutliche Einsparungen bei Fernzugriffen erzielen. Ein VPN erhöht auch die Sicherheit beim Datenaustausch. Bei der herkömmlichen Firewall-Technologie kann zwar der Inhalt der Nachricht verschlüsselt werden, nicht jedoch die Quellen- und Zieladressen. Bei der VPN-Technologie können die Benutzer eine Tunnelverbindung herstellen, bei der das gesamte Datenpaket (Header- und Datenkomponente) verschlüsselt und gekapselt ist.

Vorabregistrierung

Bei Tivoli PKI ein Prozess, mit dem ein bestimmter Benutzer (normalerweise ein Administrator) andere Benutzer registrieren kann. Wenn die Anforderung genehmigt wird, stellt die RA Informationen zur Verfügung, mit denen der Benutzer später mit Hilfe der Client-Anwendung von Tivoli PKI ein Zertifikat erhalten kann.

VPN

Virtual Private Network.

W

Web-Browser

Auf einem PC ausgeführte Client-Software, mit der ein Benutzer im World Wide Web navigieren oder lokale HTML-Seiten anzeigen kann. Der Web-Browser ist ein Abfrage-Tool, das universellen Zugriff auf die umfangreichen Hypermedia-Datensammlungen ermöglicht, die im Web und im Internet zur Verfügung gestellt werden. Manche Browser können Text und Grafik anzeigen, während andere Browser auf die Textanzeige beschränkt sind. Die meisten Browser unterstützen die Hauptformen der Internet-Kommunikation, z. B. die Ausführung von FTP-Transaktionen.

Web-Server

Ein Server-Programm, das auf Anforderungen von Browser-Programmen nach Informationsressourcen antwortet. *Siehe auch* Server.

WebSphere Application Server

Ein IBM Produkt, das Benutzer bei der Entwicklung und Verwaltung von Websites mit einem hohen Leistungsumfang unterstützt. Es erleichtert den Übergang vom einfachen Web Publishing zu komplexen e-business-Anwendungen im Web. Der WebSphere Application Server besteht aus einer Java-Servlet-Maschine, die unabhängig vom Webserver und dem verwendeten Betriebssystem arbeitet.

World Wide Web (WWW)

Der Teil des Internets, in dem ein Netz von Verbindungen zwischen Computern aufgebaut wird, auf denen Hypermediamaterial gespeichert ist. Dieses Material stellt neben Informationen auch Verbindungen (Hyperlinks) zu anderem Material im World Wide Web und Internet zur Verfügung. Der Zugriff auf WWW-Ressourcen erfolgt über einen Web-Browser.

X

X.500

Ein Standard für die Implementierung eines multifunktionalen, verteilten und vielfältigen Verzeichnisservices durch die Verbindung von Computersystemen. Dieser Standard wurde gemeinsam definiert von der bisher als CCITT bekannten International Telecommunications Union (ITU) sowie der International Organization for Standardization und der International Electro-Chemical Commission (ISO/IEC).

X.509 Version 3-Zertifikat

Das X.509v3-Zertifikat verfügt über erweiterte Datenstrukturen für die Speicherung und das Abrufen von Informationen zu Zertifikatsanträgen, zur Zertifikatsverteilung und zu Zertifikatswiderrufen sowie zu Sicherheitsregeln und digitalen Unterschriften.

X.509v3-Prozesse dienen zum Erstellen von CRLs mit Zeitmarken für alle Zertifikate. Bei jeder Verwendung eines Zertifikats ermöglichen die X.509v3-Funktionen der Anwendung, die Gültigkeit des Zertifikats zu überprüfen. Die Anwendung kann außerdem feststellen, ob sich das Zertifikat auf der Zertifikatswiderrufsliste (CRL) befindet. CRLs unter X.509v3 können für eine bestimmte Gültigkeitsperiode erstellt werden. Sie können auch auf

anderen Kriterien basieren, die zur Aufhebung der Gültigkeit eines Zertifikats führen. Wenn z. B. ein Mitarbeiter ein Unternehmen verlässt, wird sein Zertifikat in der CRL eingetragen.

X.509-Zertifikat

Ein weit verbreiteter Zertifikatsstandard, der entwickelt wurde, um die sichere Verwaltung und Verteilung von digital unterzeichneten Zertifikaten über sichere Internet-Netze zu unterstützen. Das X.509-Zertifikat definiert Datenstrukturen, die Prozeduren für die Verteilung öffentlicher Schlüssel unterstützen, die von zuverlässigen Stellen digital unterzeichnet sind.

Z

Zertifikatsaussteller (CA)

Die Software, die zur Einhaltung der Sicherheitsregeln eines Unternehmens und zur Vergabe gesicherter elektronischer Identitäten in Form von Zertifikaten dient. Der CA verarbeitet die Anforderungen von RAs zum Ausstellen, Erneuern und Widerrufen von Zertifikaten. Er kooperiert mit der RA, um Zertifikate und CRLs im Directory zu publizieren. *Siehe auch* Digitales Zertifikat.

Zertifikatserweiterung

Eine Zusatzfunktion des X.509v3-Zertifikatsformats, die zur Einbindung zusätzlicher Felder in das Zertifikat dient. Es stehen Standard- und benutzerdefinierte Erweiterungen zur Verfügung. Die Standarderweiterungen dienen verschiedenen Zwecken und umfassen Schlüssel- und Regelinformationen, Betreff- und Ausstellerattribute sowie Einschränkungen, die für den Zertifizierungspfad gelten.

Zertifikatsprofil

Eine Gruppe von Kenndaten, die den gewünschten Zertifikatstyp definieren (z. B. SSL- oder IPSec-Zertifikate). Das Profil vereinfacht die Zertifikatsspezifikation und -registrierung. Der Aussteller kann die Namen der Profile ändern und Kenndaten des gewünschten Zertifikats angeben. Hierzu zählen z. B. der Gültigkeitszeitraum, die Verwendung von Schlüsseln, DN-Einschränkungen usw.

Zertifikatsregel

Eine benannte Gruppe mit Regeln, die angibt, ob ein Zertifikat für eine bestimmte Klasse von Anwendungen mit gemeinsamen Sicherheitsanforderungen anwendbar ist. Eine Zertifikatsregel kann z. B. angeben, ob ein bestimmter Zertifizierungstyp dem Benutzer die Ausführung von Transaktionen für Waren innerhalb eines bestimmten Preisbereichs ermöglicht.

Zertifikatswiderrufsliste (CRL)

Eine digital unterzeichnete, mit Zeitmarken versehene Liste der Zertifikate, die vom Zertifikatsaussteller (CA) widerrufen wurden. Die Zertifikate in dieser Liste sollten als nicht akzeptierbar behandelt werden. *Siehe auch* Digitales Zertifikat.

Zertifizierung

Der Prozess, bei dem eine zuverlässige, an der Kommunikation nicht beteiligte Stelle (der Zertifikatsaussteller - CA) einen elektronischen Identitätsnachweis ausstellt, der für die Identität einer Person, eines Unternehmens oder einer Organisation bürgt.

Ziel

Eine benannte oder ausgewählte Datenquelle.

Zugriffssteuerungsliste (ACL)

Ein Verfahren, mit dem die Verwendung einer bestimmten Ressource auf berechtigte Benutzer beschränkt werden kann.

Index

A

Abfrageantwort 56
ACL 38
afservice.PolicyExit, Eintrag 11
Aktionen für Domäne, RA 66
Aktueller Status 67
Anforderungsattribute 65
Anforderungsprofil 40
Anforderungsstatus 67
Anpassbare Elemente 42
 Anzeigenamen für Zertifikatstypen 14
 Benachrichtigungsbrief 9
 RA Desktop, angezeigte URL-Adresse nach dem Verlassen 16
 Regel-Exit 11
 Registrierung 6
 Registrierungsauswahlliste 8
 Registrierungsbildmaterial 9
 Registrierungsfeld 7
 Registrierungsfunktion 19
 Registrierungstext 9
 Registrierungsverbindungen 10
 Zertifikatsprofil 13, 15
 Zertifikatstypbeschreibungen 13, 14, 15
Anpassung
 planen 5
 Regel-Exit 11
 Registrierung 6
 Schlüsselsicherung und -wiederherstellung 16
 Tools 41
 verwendete Dateiadressen 42
 Zertifikate 12
Anpassungs-Tasks
 Abhängigkeiten 19
 Anforderungsinformationen ändern 17
 Anzeigenamen für Zertifikatstyp ändern 14
 Automatisierung, Wartestatus 10
 Benutzererweiterungen hinzufügen 15
 Directory-Einträge 6
 Directory-Einträge erstellen 6
 Genehmigung automatisieren 10, 17
 Inaktivieren der Schlüsselsicherung und -wiederherstellung 16
 planen 5
 Regel-Exit hinzufügen 11
 Registrierungsbildmaterial hinzufügen 9
 Registrierungsfeld hinzufügen 7
 Status 'Erneuerbar' automatisch definieren 10
 Status 'Nicht erneuerbar' automatisch definieren 10
 Systemwiederanlauf erforderlich 19
 URL-Adresse für RA Desktop ändern 16
 Zertifikatsprofil ändern 13
 Zertifikatsprofil hinzufügen 13
 Zertifikatsprofil löschen 15

Anpassungs-Tasks (*Forts.*)
 Zertifikatstyp umbenennen 14
 Zertifikatstypbeschreibung ändern 14
 Zertifikatstypbeschreibung hinzufügen 13
 Zertifikatstypbeschreibung löschen 15
 zu Auswahlliste hinzufügen 8
Anpassungsbeispiel 69
Anpassungsplanung 19
Anzeigenamen, Zertifikatstyp
 ändern 14
Approver Framework 55
Attribute
 Anforderungen oder Zertifikate 65
 benutzerdefinierte Erweiterungen 64
 Datenbanksatz 24
 Zertifikatserweiterungen 28, 64
Ausführungsstatus 67
Auswahlliste, Werte hinzufügen 8
Authentifizierung 39
auto_approve, Beispiel-Exit
 ändern 11
 Beispielliste 49
 Einschränkungen 21, 22
 ersetzen 12

B

Beispieldateien 44
Benachrichtigungsbrief ändern 9
Benutzerdefinierte Erweiterungen 64
Benutzererweiterungen, zum Zertifikatsprofil hinzufügen 15
Berechtigung 39
Berechtigungen für Domäne 66
Beschädigter Schlüssel 62
Beschreibung, Zertifikatstyp
 ändern 14
 Datei 44
 hinzufügen 13
 löschen 15
Bildmaterial, für Registrierung hinzufügen 9
Brief, E-Mail-Benachrichtigung 46
Browser
 Registrierungsformularfelder 56
 Szenario für die Vorabregistrierung 21
Browser-Unterstützung 21
Browser-Zertifikat 27

C

CA-Hierarchie 25
CA-Name 54
CA-Zertifikat 27
CAs 26
certificate_profiles.cfg 45
CertTypes.jsp 44
CRL, Zertifikat entfernen 62
CRLs 26

D

Dateiadressen 42
Dateibenennung, Windows NT 41
Dateien, Beispiel 44
Dateien, Konfiguration 45, 51
Dateitypen, Anpassung 41
Daten, Registrierung 65
Datenbanksätze
 Attribute 24
 Verarbeitung durch RA 3
DB2 24
Debug-Stufe 51
Digitales Zertifikat 27
 Anforderung 3
 angebotenen Typ umbenennen 14
 anpassen 12
 Benutzererweiterungen zum Profil hinzufügen 15
 Datenbanksatz 24
 Einzeldaten 62
 erneuerbar 27
 Erneuerbarkeit 28
 Gültigkeitsdauer 25, 27
 Profil ändern 13
 Profil hinzufügen 13
 Profil löschen 15
 registrierter Name 26
 Status 67
 Verwaltung 38
 X.509v3-Format 64
 zur Verwendung der Registrierungsservices 27
Domäne, Regeln für 23
Domäne, Registrierung 24

E

E-Mail-Benachrichtigungsbrief 46
 Brief ändern 9
 Dateiname 53
 Feld 56
E-Mail-Ersetzungsvariablen 46
Einheitenzertifikat 28
Einschränkungen bei Regel-Exits 21
Elemente, anpassbare 42
Erläuterungen, Themen 19
Erneuerbares Zertifikat, automatisch definieren 10

Erneuerbarkeit 28
Erneuerbarkeitsstatus, automatisch 10
Ersetzungsvariablen für E-Mail 46
Erweiterungen, benutzerdefinierte zum Zertifikat hinzufügen 15
Erweiterungen, X.509v3-Zertifikat 28, 64

F

Fehlernachrichtentext 47
Felder für Registrierung 66
 hinzufügen 7

G

Gegenseitige Zertifizierung 25
Genehmigung 3
Genehmigung automatisieren 10, 17
Geschäftsprozess, Schablonendatei 55
Gründe für Widerruf 62
Gültigkeitszeitraum 40, 62

I

Informationen zur Vorgehensweise, Themen 5
Inhalt des Handbuchs ix

J

Java Server-Seiten 24
 Beispiel 48
 Dateinamendefinitionen 52
 Liste 43, 48
JSP-Dateien 43, 48, 52

K

Klassen für Schemaobjekte angeben 36
Klassen von Objekten für Verzeichniseinträge anpassen 114
Konfigurationsdateien 45, 51
Konventionen xi
Kundenunterstützung xi

L

LDAP-Protokoll 26

M

Mehrere Administratoren 39
Mount-Punkte 52

N

Nicht erneuerbares Zertifikat, automatisch definieren 10

O

Objektklassen für Schemata angeben 36
Objektklassen für Verzeichniseinträge anpassen 114

P

PKCS #10-Zertifikatsanforderung 28, 56
PKCS #12-Datei wiederherstellen 40
PKCS #7-Zertifikat 28, 56
PKIX-kompatible Anwendung 27
Planen der Anpassung 5, 19
Profil, Anforderung 40
Profile, Zertifikat 29
Protokoll für den Verzeichniszugriff (Directory) 26
Protokolle für die gesicherte Kommunikation 27

R

RA 24
RA Desktop 38, 39
 angezeigte URL-Adresse nach dem Verlassen ändern 16
 Servlet zur Unterstützung 39
RA Desktop, Konfigurationsdatei 54
RA Desktop, URL-Adresse 55
RA-Server, Aktionstabelle 54
RA-Server, URL-Adresse 52
RA-Server-Parameter 54
raconfig.cfg 51
Referenzinformationen, Themen 41
Regel, Unternehmen 23
Regel-Exits
 anpassen 11
 Beispiel-Exit ändern 11
 Beispiel-Exit ersetzen 12
 Beispieldatei 49
 Einschränkungen 21, 22
 Genehmigung automatisieren 10
 hinzufügen 11
 in raconfig.cfg angeben 11
 Status 'Erneuerbar' automatisch definieren 10
 Status 'Nicht erneuerbar' automatisch definieren 10
 Wartestatus automatisch definieren 10
Registrator 39

Registrator (*Forts.*)
 Aktionen von 66
 Aufgabenbereich 3
 Auswirkungen auf die Registrierungsdatenbank 25
 automatische Tasks 3, 23
 Berechtigungen für Domäne 66
 mehrere Administratoren 39
 Servlet zur Unterstützung von Tasks 39
Registrierter Name 26
Registrierung 3, 6, 23
 Aktionen für 66
 automatische 3, 23
 benötigte Regeln 24
 Notwendigkeit 3
 Tasks des Registrators 3
 Unternehmensregel anwenden 23
 Web-Browser-Unterstützung 21
Registrierungs-Web-Seiten 20, 43, 48
 CA-Zertifikat für die Verwendung 27
 Felder für die Zertifikatsanforderung 59
 Felder für Registrierungsinformationen 56
 Java Server-Seiten 48
 Zweck 20
Registrierungsanforderung
 auswerten 23
 automatische Auswertung 23
 Datenbanksatz 25
 Gültigkeitsdauer 25
 Registrierungsformular 19
 Status 67
 Verarbeitung durch RA 3
 verwendete Profile 40
 Vorabregistrierung 19, 21
 Web-Browser-Unterstützung 21
 Web-Seiten 20
Registrierungsattribute 65
Registrierungsdaten 65
Registrierungsdatenbank 3, 24
 Zugriffseintrag 51
Registrierungsdomäne 3, 24, 39
Registrierungsformular, Felder
 hinzufügen 7
Registrierungsformularfelder 56, 66
Registrierungsfunktion 20
 anpassbare Elemente 19
 Bildmaterial hinzufügen 9
 Konfigurationsdatei 51
 URL-Adresse 10
 Verbindung herstellen 10
Registrierungsfunktion, definiert 3
Registrierungsinformationen, Felder 56
Registrierungssätze 25
 Attribute 24
 Verarbeitung durch RA 3
Registrierungsstelle 24
Registrierungstext ändern 9
Registrierungstypen 19

S

- Schemaobjektklassen angeben 36
- Schlüssel, beschädigt 62
- Schlüsselsicherung und -wiederherstellung
 - automatische Genehmigung 17
 - Beschreibung 40
 - Genehmigung automatisieren 17
 - inaktivieren 16
- Schlüsselwiederherstellung 16, 40
- Schnittstellen zum Regel-Exit 22
- Server-Zertifikat 28
- Servlet zur Unterstützung von RA Desktop 39
- Sichere Anwendungen 3
- Sicherung und Wiederherstellung von Schlüsseln 16, 40
- Status, Anforderung 67
- Status, Ausführung 67
- Statuswerte 67
- Systemwiederanlauf 19
- Szenario für die Vorabregistrierung 21

T

- Text, Ändern für Registrierung 9
- Tivoli
 - Kundenunterstützung xi
 - Sicherheitsverwaltung - Webinformationen xi
- Tivoli PKI
 - Webinformationen xi
- Tivoli PKI, Wiederanlauf 19
- Tivoli PKI-Client-Anwendung 19
- Tools für die Anpassung 41
- Typen von Zertifikaten 62

U

- Übersicht
 - Aufgabenbereich des Registrators 3
 - Tivoli PKI 1
- Unternehmensregel 23
- Unterstützung für Tivoli-Kunden xi
- URL-Adresse
 - nach dem Verlassen von RA Desktop 16
 - Registrierungsdomäne 24
 - Registrierungsfunktion 10

V

- Verarbeitungsattribute 65
- Verlassen, URL-Adresse, für RA Desktop ändern 16
- Veröffentlichungen
 - Tivoli-Sicherheitsprodukte xi
- Verzeichniseinträge, Objektklassen anpassen 114
- Verzeichnisname (Directory) 54
- Verzeichnisstruktur 42

- Verzeichniszugriff (Directory) 26
- Vorabregistrierungsszenario 21
- Vorwort ix

W

- Wartestatus, automatisch 10
- Wartestatus, für Zertifikat definieren 62
- Web-Browser
 - Registrierungsformularfelder 56
 - Szenario für die Vorabregistrierung 21
- Web-Browser-Unterstützung 19, 21
- Web-Seiten, Registrierung 20, 43, 48
 - CA-Zertifikat für die Verwendung 27
 - Felder für die Zertifikatsanforderung 59
 - Felder für Registrierungsinformationen 56
 - Java Server-Seiten 48
 - Zweck 20
- Web-Seitenelemente 56
- Website für
 - Sicherheitsverwaltungsinformationen xi
 - Tivoli-Kundenunterstützung xi
 - Tivoli Public Key Infrastructure xi
 - Tivoli-Sicherheitsprodukte xi
- WebSphere 1
- Wert, zu Auswahlliste hinzufügen 8
- Widerruf, Gründe 62
- Wiederherstellung von Schlüsseln 16, 40
- Windows NT, Dateibenennung 41

X

- X.509v3-Zertifikatserweiterungen 28, 64
- X.509v3-Zertifikatsformat 64

Z

- Zertifikat 27
 - Anforderung 3
 - angebotenen Typ umbenennen 14
 - anpassen 12
 - Benutzererweiterungen zum Profil hinzufügen 15
 - Datenbanksatz 24
 - Einzeldaten 62
 - erneuerbar 27
 - Erneuerbarkeit 28
 - Gültigkeitsdauer 25, 27
 - Profil ändern 13
 - Profil hinzufügen 13
 - Profil löschen 15
 - registrierter Name 26
 - Status 67
 - Verwaltung 38
 - X.509v3-Format 64
 - zur Verwendung der Registrierungsservices 27

- Zertifikatsanforderung, Felder 59
- Zertifikatsattribute 65
- Zertifikatsaussteller 26
- Zertifikatserweiterungen 15, 28, 64
- Zertifikatskategorien 27
- Zertifikatsprofil 29
 - ändern 13
 - Benutzererweiterungen hinzufügen 15
 - hinzufügen 13
 - Konfigurationsdatei 45, 53
 - löschen 15
 - vektorspezifisch 53
- Zertifikatstyp 62
 - Anzeigename ändern 14
 - Beschreibung ändern 14
 - Beschreibung löschen 15
 - Beschreibungsdatei 44
 - neue Beschreibung hinzufügen 13
- Zertifikatswiderrufsliste 26
- Zertifizierung 25
- Zertifizierungshierarchie 25
- Zielgruppe ix
- Zugriffssteuerungsliste 38
- Zusammenfassung
 - verwendete Konventionen xi
- Zweck des Zertifikats 62



SH12-3000-02

